

Шестое Издание

Руководство #1  
во всем мире  
по развертыванию  
Wi-Fi

# CWNA®

Сертифицированный  
Администратор  
Беспроводных Сетей

## УЧЕБНОЕ ПОСОБИЕ

ЭКЗАМЕН CWNA-108

Включает интерактивную онлайн среду и инструменты обучения:

Более 500 тренировочных вопросов

300 электронных карточек для запоминания

Словарь ключевых терминов с поиском

ДЭВИД Д. КОУЛМЕН

CWNE #4

ДЭВИД А. УЕСТКОТТ

CWNE #7

 SYBEX®  
A Wiley Brand



**CWNA®**

**Сертифицированный  
Администратор  
Беспроводных Сетей**

**Учебное Пособие**

**Шестое Издание**





**CWNA®**

# **Certified Wireless Network Administrator**

## **Study Guide**

### **Exam CWNA-108**

### **Sixth Edition**



David D. Coleman, CWNE #4

David A. Westcott, CWNE #7

Copyright © 2021 by John Wiley & Sons, Inc., Индианаполис, Индиана

Опубликовано одновременно в Канаде и в Соединенном Королевстве

ISBN: 978-1-119-73450-5

ISBN: 978-1-119-73633-2 (ebk.)

ISBN: 978-1-119-73453-6 (ebk.)

Никакая часть этой публикации не может быть воспроизведена, сохранена в информационно-поисковых системах или передана в любой форме или любым способом, электронно, механически, фотокопированием, записью, сканированием или иным способом, за исключением того как разрешено в Разделе 107 или 108 Закона об Авторском Праве Соединенных Штатов 1976 года, без или более раннего письменного разрешения Издателя, или авторизации путем оплаты соответствующей стоимости за копию в Центр по Разрешению Авторских Прав, 222, Розевуд Драйв, Дэнверс, MA 01923 [Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923], (978) 750-8400, факс (978) 646-8600. Запросы к Издателю за разрешением должны быть адресованы в Отдел Разрешений, Джон Вайли и Сыновья Инк., 111 Ривер Стрит, Обокен, Нью Джерси 07030 [Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030], (201) 748-6011, факс (201) 748-6008, или онлайн на сайте [www.wiley.com/go/permissions](http://www.wiley.com/go/permissions).

**Ограничение Ответственности/Отказ от Гарантии:** Издатель и автор не делают никаких заявлений или гарантий в отношении точности или полноты содержания этой работы и, в частности, отказываются от каких-либо гарантий, включая помимо прочего гарантии пригодности для определенной цели. Никакая гарантия не может быть создана или расширена путем продажи или с помощью рекламных материалов. Совет и стратегии, содержащиеся здесь, могут не быть подходящими для каждой ситуации. Эта работа продается с подразумеванием того, что издатель не вовлечен в оказание юридических, бухгалтерских или иных профессиональных услуг. Если требуется профессиональная помощь, следует обратиться к услугам компетентного профессионального человека. Ни издатель, ни автор не ответственны за убытки исходящие отсюда. Факт того, что организация или вебсайт указан в этой работе в качестве цитаты и/или потенциального источника для дальнейшей информации не означает, что автор или издатель поддерживают информацию, которую организация или веб сайт могут предоставить, или рекомендации, который они могут дать. Кроме того, читателям следует знать, что Интернет вебсайты, перечисленные в этой работе могут измениться или пропасть, между тем как работа писалась и когда ее читают.

За общей информацией по нашим продуктам и услугам, или для получения технической поддержки, обращайтесь в Отдел Поддержка Заказчиков внутри США по телефону +1 (877) 762-2974, за пределами США по телефону +1 (317) 572-3993 или по факсу +1 (317) 572-4002.

Wiley публикует в различных печатных и электронных форматах, и печати по запросу. Некоторые материалы, включенные в стандартную печатную версию этой книги может быть не включена в электронные книги [e-books] или в книги напечатанные по запросу [print-on-demand]. Если книга ссылается на материалы на CD или DVD, которые не включены в версию, которую вы купили, вы можете загрузить эти материалы с [booksupport.wiley.com](http://booksupport.wiley.com). За дополнительной информацией по продуктам Wiley посетите [www.wiley.com](http://www.wiley.com).

**Контрольный Номер Библиотеки Конгресса:** 2020951883

**ТОРГОВЫЕ МАРКИ:** Wiley, логотип Wiley, и логотип Sybex являются торговыми марками или зарегистрированными торговыми марками John Wiley & Sons, Inc. и/или их филиалов, в Соединенных Штатах и других странах, и не могут быть использованы без письменного разрешения. CWNA является зарегистрированной торговой маркой CWNP, LLC. Все другие торговые марки являются собственностью из соответствующих владельцев. John Wiley & Sons, Inc. не связан ни с каким продуктом или производителем, упомянутыми в этой книге.

---

“Инвестиции в знания всегда приносят наибольший процент.”

Бенжамин Франклайн, один из Отцов Основателей Соединенных Штатов

---

*Почти 17 лет назад мы были подведены нашим издателем к соавторству учебного руководства для сертификационного экзамена Сертифицированный Администратор Беспроводных Сетей. В то время, фразе «Wi-Fi» было несколько лет отроду, и она только начинала проникать в нашу культуру.*

*Технология 802.11g только начала появляться, и мы были так взбудоражены адской скоростью в 54Мбит/с, доступной в частотном диапазоне 2,4Ггц. Мы согласились стать авторами книги. Шесть изданий позже, технология 802.11 WLAN радикально раскрутилась и Wi-Fi теперь неотъемлемая часть нашей повседневной жизни.*

*Сертификация CWNA долгое время считалась сертификацией базового уровня для сетевых профessionалов, думающих подтвердить свои знания технологии БЛВС 802.11. Как авторы, мы признательны десяткам тысячам людей, которые купили Учебное Пособие CWNA, чтобы помочь им в их стремлении к сертификации CWNA. Мы также признательны, что много университетов и колледжей выбрали книгу в качестве их учебного курса по классам беспроводных технологий. В наших путешествиях мы встречали и становились друзьями со многими нашими читателями прошлых пяти изданий книги. Мы обнаружили, что большое количество людей, которые купили книгу, используют ее в качестве справочного руководства на рабочем месте, а не только как учебное пособие. Также нам много людей рассказали, что книга помогла им продвинуться в их Wi-Fi карьере. Еще раз, мы очень признательны, и мы хотели бы посвятить бое издание Учебного Пособия CWNA нашим читателям.*

*Наша цель всегда была обучить как можно больше людей технологии БЛВС. Если вы новичок в беспроводных сетях 802.11, мы надеемся, что эта книга будет вашим первыми инвестициями в знания Wi-Fi. Если вы ветеран профессионал БЛВС, мы надеемся, что, когда вы закончите читать эту книгу, вы передадите ее другу или коллеге. Распространение знаний о Wi-Fi будет выгодной инвестицией.*

*Искренне ваши,*

*Дэвид Коулмен и Дэвид Уесткотт*



# Признательности

Когда мы написали первую редакцию Учебного Пособия CWNA, дети Дэвида Коулмена были маленькими детьми. Сейчас у Каролины магистерская степень по общественной политике Университета Южной Калифорнии (USC). Брэнти закончил Бостонский Университет и недавно получил свою докторскую степень (Ph.D.) по биохимии в Университете Вашингтона. Дэвид хотел бы поблагодарить своих теперь уже взрослых детей за годы поддержки и за то, что делают своего отца очень гордым. Дэвид также хотел бы поблагодарить свою мать, Маржори Барнс, приемного отца, Вильяма Барнса, и брата, Роба Коулмена, за многие годы поддержки и ободрения. Дэвид хотел бы особенно поблагодарить свою жену, Валла Анн, за то, что она приносит радость и смех в каждый день их жизни.

Дэвид Коулмен также хотел бы поблагодарить своих друзей и семью Экстрим Нетворкс (Extreme Networks [www.extremenetworks.com](http://www.extremenetworks.com)) и бывшую Аэрохайв Нетворкс (Aerohive Networks). Существует много прошлых и настоящих сотрудников Аэрохайв и Экстрим, которых он хотел бы поблагодарить, но здесь просто не хватит места. Поэтому спасибо всем его коллегам. Это был один дикий заезд за прошедшие 11 лет!

Дэвид Уесткотт хотел бы поблагодарить свою жену, Джани, за ее любовь и поддержку, и за то, что она краеугольный камень их семьи. Ее любовь и ежедневная поддержка четырех поколений семьи не осталась незамеченной и недооцененной.

Дэвид Уесткотт также хотел бы поблагодарить учебный отдел Аруба Нетворкс (Aruba Networks). В 2004 году Аруба Нетворкс наняли его в качестве первого контрактного тренера. Многое изменилось за годы, но это все еще веселое и волнующее путешествие.

Написание *CWNA: Учебного Руководства Сертифицированный Администратор Беспроводных Сетей [Certified Wireless Network Administrator Study Guide]* снова было приключением. Мы хотели бы поблагодарить следующих людей за их поддержку и вклад в течении всего процесса.

Мы должны прежде всего поблагодарить редактора Sybex по поиску текстов для издания Джима Минатела [Jim Minatel] за то, что он добрался до нас и сподвиг нас на написание этой шестой редакции нашей книги. Мы бы также хотели поблагодарить нашего редактора, Ким Уимпсетт [Kim Wimpsett], с кем было приятно работать над несколькими книжными проектами. Нам также нужно выразить особую благодарность нашему управляющему редактору Пит Гоген [Pete Gaughan]; нашему специалисту по улучшению текста Барату Кумру Раджасекарену [Barath Kumar Rajasekaran]; Элизабете Уэлч [Elizabeth Welch] нашему корректору; и Луизе Уотсон [Louise Watson], нашему финальному корректору.

Нам также нужно выразить горячую благодарность нашему техническому редактору Бену Уилсону [Ben Wilson] из Фортинет [Fortinet] ([www.fortinet.com](http://www.fortinet.com)). Бен накопил годы Wi-Fi опыта, работая на трех основных производителей БЛВС. Обратная связь и данные предоставленные Беном были бесценны.

Особую благодарность мы должны выразить Эндрю фон Наги [Andrew von Nagy] CWNE #84 и Марко Бертону [Marcus Burton], CWNE #78, за их экспертизу в качестве технических редакторов в ранних изданиях книги.

Эндрю Крокер [Andrew Crocker] снова обеспечил нас удивительными фотографиями и потрясающим монтажом некоторых не очень удивительных фотографий, которые мы ему предоставили. Вы можете увидеть больше его работ или талантов на [www.andrewcrocker.photography](http://www.andrewcrocker.photography).

Спасибо Proxim и Кену Раппелу [Ken Ruppel] ([kenrappel@gmail.com](mailto:kenrappel@gmail.com)) за то, что позволили включить видеоролик *Модели Лучей и Поляризация Направленных Антенн*

X

[*Beam Patterns and Polarization of Directional Antennas*] в онлайн ресурсы книги, которые доступны по адресу [www.wiley.com/go/cwnasg6e](http://www.wiley.com/go/cwnasg6e).

Особая благодарность Андрасу Силағы [Andras Szilagyi] за создание веб приложения EMANIM, которое используется в качестве упражнений в Главе 3 “Основы Радиотехники”. Вы можете связаться с Андрасом по адресу [www.szialab.org](http://www.szialab.org).

Спасибо Крису деПуи [Chris DePuy] из технологической исследовательской фирмы Группа 650 [650 Group] ([www.650group.com](http://www.650group.com)) за аналитику отрасли БЛВС.

Благодарим Марко Тислера [Marko Tisler], CWNE #126, за его вклад в содержание о APIs. Благодарим Грегора Вукайк [Gregor Vucajn], CWNE #96, за его копию касательно LTE. Спасибо Карлу Бенедикту [Karl Benedict] за его данные и материалы о направленных антennaх. Спасибо Перри Корреллу [Perry Correll] за его данные относительно 802.11ax и Wi-Fi 6E.

Самая большая благодарность Рику Мерфи [Rick Murphy], CWNE #10, за его материалы касательно OFDM. Рик предлагает выдающиеся учебные ресурсы по БЛВС по адресу [howwirelessworks.com](http://howwirelessworks.com).

Самая особенная благодарность Адриану Гранадосу [Adrian Granados] за весь его вклад в беспроводное сообщество. Обязательно ознакомьтесь с его крутыми Wi-Fi приложениями на [www.intuitibits.com](http://www.intuitibits.com).

Мы должны горячо поблагодарить Ли Бэдмена [Lee Badman], CWNE #200, за его пародийные блоги и мемы, которые он создал по последнему изданию этой книги. (Он также пишет великолепные технические блоги.)

Некоторые другие рок звезды БЛВС упоминаемые в этом экземпляре этой книги: Сэм Клементс [Sam Clements], CWNE #101; Найджел Боуден [Nigel Bowden], CWNE #135; Майк Альбано [Mike Albano], CWNE #150; Эдди Фореро [Eddie Forero], CWNE #160; Джеймс Гарринджер [James Garringer], CWNE #179; Глен Кейт [Glen Cate], CWNE #181; Джером Хенри [Jerome Henry], CWNE #45; Франсуа Верже [François Vergès], CWNE #180; Роуэлл Дионисио [Rowell Dionicio], CWNE #210; Мэнон Лессард [Manon Lessard], CWNE #275; Фил Морган [Phil Morgan], CWNE #322; Мак Деринг [Mac Deryng], CWNE #357, и Мэтт Старлинг [Matt Starling], CWNE #369.

Мы также хотели бы поблагодарить следующих людей и компаний за их поддержку и вклад в эту книгу:

Девин Акин [Devin Akin], CWNE #1, из Дивергент Дайнэмикс [Divergent Dynamics] ([www.divdyn.com](http://www.divdyn.com))

Дэннис Буррелл [Dennis Burrell], Технолог Продуктовых Инноваций в Вентев [Ventev] ([www.ventev.com](http://www.ventev.com))

Келли Берроуз [Kelly Burroughs], Менеджер Продуктового Маркетинга в айБэйв [iBwave] ([www.ibwave.com](http://www.ibwave.com))

Майк Чирелло [Mike Cirello], Сооснователь ХайвРэйдар [HiveRadar] ([www.hiveradar.com](http://www.hiveradar.com))

Джейми Фабрегас Фернандес [Jaime Fábregas Fernández], Менеджер R&D в Тарлоджик Рисеч С.Л. [Tarlogic Research S.L.] ([www.acrylicwifi.com](http://www.acrylicwifi.com))

Тина Ханзлик [Tina Hanzlik], Директор по Маркетинговым Коммуникациям, и Кари Айсслер, Старший Менеджер по Маркетинговым Коммуникациям Wi-Fi Альянса [Wi-

Fi Alliance] ([www.wi-fi.org](http://www.wi-fi.org))

Джеймс Какоска [James Kahkoska], СТО НетАлли [NetAlly] ([www.netally.com](http://www.netally.com))

Брайан Лонг [Brian Long], CWNE #159, Вице Президент, Глобальные

Профессиональные Услуги и Обучение в Масимо [Masimo] ([www.masimo.com](http://www.masimo.com))

Тауни Одия [Tauni Odia], Директор Продуктового Маркетинга в Екахай

[Ekahau] ([www.ekahau.com](http://www.ekahau.com))

Скотт Томпсон [Scott Thompson], Президент Оберона [Oberon, Inc.]

([www.oberoninc.com](http://www.oberoninc.com))

Райан Вудингс [Ryan Woodings], Основатель МетаГик [ MetaGeek] ([www.metageek.com](http://www.metageek.com))

Мы также хотим поблагодарить Кейта Парсонса [Keith Parsons], CWNE #3, и его команды в wirelessLAN Professionals. Кейт построил всемирное сообщество экспертов БЛВС, которые делятся знаниями. Вы можете узнать больше о конференциях Профессионалы беспроводныхЛВС [wirelessLAN Professionals] по адресу [www.wlanprofessionals.com](http://www.wlanprofessionals.com).

Мы бы также хотели поблагодарить Тома Карпентера [Tom Carpenter], CWNE #104, из программы CWNP ([www.cwnp.com](http://www.cwnp.com)). Все сотрудники CWNP, прошлые и настоящие, должны гордиться всемирно известной программой сертификации по беспроводной связи, которая задает образовательный стандарт на предприятиях Wi-Fi отрасли. Было очень приятно работать со всеми вами последние два десятилетия.

Наконец, мы бы хотели поблагодарить Марка Хунга [Mark Hung], Вице Президента по Технологии и Инжинирингу в Wi-Fi Альянсе, за заставляющее задуматься предисловие, которое он написал для этой книги.



# Об Авторах

**Дэвид Д. Коулмен [David D. Coleman]** Директор Маркетинга Продуктов Экстрим Нетворкс [Extreme Networks ([www.extremenetworks.com](http://www.extremenetworks.com))]. Дэвид – публичный докладчик и искусный технический автор, который специализируется на Wi-Fi и облачных технологиях, он член команды Технических Евангелистов компании Экстрим Нетворкс. Дэвид путешествует по миру для встреч с заказчиками и с партнерами, на форумы, на обучающие тренинги. Он инструктировал ИТ профессионалов по всему миру по дизайну Wi-Fi, безопасности, администрированию, устранению проблем.

Дэвид написал много книг, блогов, и информационных листовок («white papers») по беспроводным сетям, и он считается авторитетным источником по технологии 802.11. До работы в Экстрим он специализировался на корпоративном и государственном тренинге и консалтинге по Wi-Fi. В прошлом, он оказывал консультации по Wi-Fi большому количеству частных корпораций, военным США, и другим федеральным и государственным агентствам. Дэвид также является получателем Награды за достижения в WiFi в 2020 году: Wi-Fi Lifetime Achievement Award ([www.thewifiawards.com/2020-award-winners](http://www.thewifiawards.com/2020-award-winners)). Когда он не путешествует, он находится в Атланте, Джорджия и на Озере Чапала, Мексика со своей женой Валлой Анн. Дэвид – CWNE#4 и с ним можно связаться по электронной почте [mistermultipath@gmail.com](mailto:mistermultipath@gmail.com). Следуйте за Дэвидом на Твиттере (Twitter): @mistermultipath.

**Дэвид А. Уесткотт [David A. Westcott]** независимый консультант и технический тренер с более чем 35 летним опытом. Он сертифицированный тренер более 28 лет и специализируется на беспроводных сетях, управлении и мониторинге беспроводных сетей, управление сетевым доступом. Он проводит тренинги для тысяч студентов в государственных агентствах, корпорациях и университетах в более чем 30 странах по всему миру. Дэвид был членом преподавателей, работающих по контракту в Корпоративном Образовательном Центре Бостонского Университета более 10 лет. Он является автором: Осмысление ArubaOS: Версия 8.x (Understanding ArubaOS: Version 8.x (Bowker, 2019)) и Осмысление ArubaOS: Версия 6.x (Understanding ArubaOS: Version 6.x (Westcott Consulting, Inc., 2017)) и у него есть соавторство множества книг, написано множество информационных листов (White papers), разработано множество курсов по проводным и беспроводным сетевым технологиям и сетевой безопасности.

Дэвид был членом оригинального круглого стола CWNE. Он CWNE#007 и получил сертификации от многих компаний, включая Аруба Неворкс (Aruba Networks), Сильвер Пик (SilverPeak), Сиксо (Cisco), Майкрософт (Microsoft), Екахай (Ekahau), ИЭС-Коунсил (EC-Council), КомпТИА (CompTIA) и Новелл (Novell). Он живет в Конкорде, Массачусетс, со своей женой, Джани. С Дэвидом можно связаться по электронной почте [david@westcott-consulting.com](mailto:david@westcott-consulting.com). Следите за Дэвидом на Твиттере (Twitter): @davidwestcott.



## О Техническом Редакторе

**Бен Уилсон [Ben Wilson]** был связан с беспроводной связью с ее ранних коммерциализированных начинаний, работая на разных производителях и технологиях за все время. Работая в различных ролях, он установил больше точек доступа (AP) и сделал больше интеграций, чем он мог бы вспомнить, если захотел бы, за последние 20 лет. Сегодня Бен работает Вице Президентом по Управлению Проектами в Фортинет [Fortinet], где он помогает вести продуктовую стратегию, управление и развитие беспроводных и других технологий. Следите за Беном на Твиттере (Twitter): @AirNetworkBen



# Перевод на Русский Язык

Перевод на Русский Язык выполнен Елкиным Ярославом Владимировичем для своей семьи на основании приобретения книги CWNA® Certified Wireless Network Administrator Study Guide Exam CWNA-108 Sixth Edition, издательства Sybex, которое является частью издательства John Wiley & Sons. Текст перевода депонирован.



# Оглавление

<i>Предисловие</i>	<i>xxxxv</i>	
<i>Введение</i>	<i>xxxvii</i>	
<i>Оценочный Тест</i>	<i>lvi</i>	
<b>Глава 1</b>	Обзор Беспроводных Стандартов, Организаций и Основ	1
<b>Глава 2</b>	Стандарты и Поправки IEEE 802.11	45
<b>Глава 3</b>	Основы Радиотехники	85
<b>Глава 4</b>	Компоненты, Параметры и Математика Радиосвязи	123
<b>Глава 5</b>	Радиосигнал и Концепции Антенн	165
<b>Глава 6</b>	Беспроводные Сети и Технологии Расширения Спектра	219
<b>Глава 7</b>	Топологии Беспроводных ЛВС	267
<b>Глава 8</b>	Доступ к Среде 802.11	299
<b>Глава 9</b>	802.11 MAC	323
<b>Глава 10</b>	Технология MIMO: НТ и VHT	393
<b>Глава 11</b>	Архитектура БЛВС	459
<b>Глава 12</b>	Питание по Ethernet (PoE)	517
<b>Глава 13</b>	Концепции Проектирования БЛВС	551
<b>Глава 14</b>	Обследование и Контрольное обследование	631
<b>Глава 15</b>	Решение проблем БЛВС	687
<b>Глава 16</b>	Беспроводные Атаки, Мониторинг Вторжений, и Политик	757
<b>Глава 17</b>	Архитектура Безопасности Сетей 802.11	801
<b>Глава 18</b>	Приноси Свое Устройство (BYOD) и Гостевой Доступ	871

## Оглавление

xx

<b>Глава</b>	<b>19</b>	802.11ax: Высокая Эффективность (HE)	943
<b>Глава</b>	<b>20</b>	Установка БЛВС и Вертикальные Рынки	1003
<b>Приложение</b>	<b>A</b>	Ответы на Контрольные Вопросы	1035
<b>Приложение</b>	<b>B</b>	Аббревиатуры и Акронимы	1089
<i>Указатель</i>			???

# Содержание

<i>Предисловие</i>	<i>xxxv</i>	
<i>Введение</i>	<i>xxxvii</i>	
<i>Оценочный Тест</i>	<i>lvi</i>	
<b>Глава 1      1</b>	<b>Обзор Беспроводных Стандартов, Организаций и Основ</b>	<b>1</b>
	История беспроводных локальных вычислительных сетей	3
	Организации по Стандартам	6
	Федеральная Комиссия по Связи	6
	Международный Союз Электросвязи	
	Сектор Радиосвязи	7
	Институт Инженеров по Электротехнике и Электронике	10
	Подразделение Инженерных Задач Интернета	11
	Wi-Fi Альянс	13
	Международная Организация по Стандартизации	25
	Ядро, распределение и доступ	27
	Основы связи	29
	Терминология связи	29
	Понимание Несущих Сигналов	30
	Понимание Методов Кодирования	32
	Итого	39
	Темы Экзамена	39
	Контрольные Вопросы	40
<b>Глава 2      2</b>	<b>Стандарты и Поправки IEEE 802.11</b>	<b>45</b>
	Первоначальный Стандарт IEEE 802.11	48
	Принятые Поправки IEEE 802.11-2020	50
	802.11a-1999	51
	802.11b-1999	52
	802.11d-2001	53
	802.11e-2005	53
	802.11g-2003	53
	802.11h-2003	56
	802.11i-2004	58
	802.11j-2004	59
	802.11k-2008	60
	802.11n-2009	61
	802.11p-2010	61
	802.11r-2008	62
	802.11s-2011	62
	802.11u-2011	64

## Содержание

*xxii*

802.11v-2011	65
802.11w-2009	65
802.11y-2008	66
802.11z-2010	66
802.11aa-2012	66
802.11ac-2013	66
802.11ad-2012	67
802.11ae-2012	68
802.11af-2014	68
802.11ah-2016	69
802.11ai-2016	70
802.11aj-2018	70
802.11ak-2018	70
802.11aq-2018	70
Черновые Поправки IEEE 802.11	70
802.11ax (High Efficiency)	71
802.11ay (Next-Generation 60 GHz)	72
802.11az (Next-Generation Positioning)	72
802.11ba (Wake-Up Radio)	72
802.11bb (Light Communications)	72
802.11bc (Enhanced Broadcast Service)	72
802.11bd (Enhancements for Next-Generation V2X)	73
802.11be (Extremely High Throughput)	73
Нерабочие Поправки	73
802.11F	73
802.11T	75
IEEE Рабочая Группа по Задаче m	76
Итого	77
Темы Экзамена	77
Контрольные Вопросы	79
<b>Глава 3 Основы Радиотехники</b>	<b>83</b>
Что такое радиочастотный сигнал?	86
Характеристики радиоволн	86
Длина волны	88
Частота	93
Амплитуда	94
Фаза	95
Поведение радиоволн	96
Распространение волн	96
Поглощение	97
Отражение	98
Рассеивание	100
Рефракция	100
Дифракция	101
Потери (Затухание)	103

	Ослабление на пути в Свободном Пространстве	105
	Многолучевое распространение	107
	Усиление	122
	Инструменты радиоанализа	113
Глава 4	Итого	114
	Темы Экзамена	114
	Контрольные вопросы	116
<b>Глава 4</b>	<b>Компоненты, Параметры и Математика Радиосвязи</b>	<b>121</b>
	Компоненты радиосвязи	124
	Передатчик	124
	Антenna	125
	Приемник	126
	Расчетный излучатель	126
	Эквивалентная Изотропно Излучаемая Мощность	126
	Единицы Мощности и Сравнения	128
	Ватт	129
	Милливатт	129
	Децибел	130
	Децибели относительно изотропного излучателя (дБи)	133
	Децибели относительно полуволновой дипольной антенны (дБд)	133
	Децибели относительно 1 милливатта (дБм)	134
	Закон обратных квадратов	135
	Радиоволновая математика	136
	Правило десяток (10) и троек (3)	137
	Краткий итог по радиоволновой математике	142
	Уровень Шума	143
	Отношение Сигнал-Шум	143
	Отношение Сигнала к Интерференции плюс Шум	144
	Индикатор Силы Принятого Сигнала	144
	Бюджет Линии Связи	150
	Запас на замирание/Рабочий Запас Систем	153
	Итого	155
	Темы Экзамена	157
	Контрольные Вопросы	158
<b>Глава 5</b>	<b>Радиосигнал и Основы Теории Антенн</b>	<b>163</b>
	Диаграммы направленности по Азимуту и Углу Места (Огибающая Излучения Антennы)	166
	Чтение Полярных Диаграмм	168
	Ширина луча	171
	Типы Антенн	173
	Всенаправленные Антennы	177
	Всенаправленные антennы с наклоном вниз	179
	Полунаправленные Антennы	178
	Узконаправленные Антennы	180
	Секторные Антennы	182

Антенные Решетки	183
Линия Прямой Видимости	185
Радиоволновая Линия Прямой Видимости	186
Зона Френеля	186
Изгиб Земли	191
Поляризация Антенн	192
Разнесение Антенн	193
Много Вводов, Много Выводов (MIMO)	194
Антенные МИМО	195
Установка и Соединение Антенн	196
Коэффициент Стоячей Волны по Напряжению	196
Затухание Сигнала	198
Установка Антennы	199
Антенные Аксессуары	206
Кабели	206
Разъемы	207
Делители	207
Усилители	208
Аттенюаторы	209
Грозоразрядники	209
Заземляющие стержни и провода	210
Соответствие Нормативам	211
Итого	212
Темы Экзамена	212
Контрольные Вопросы	213
<b>Глава 6 Беспроводные Сети и Технологии Расширения Спектра</b>	<b>217</b>
Пропускная способность против Ширины полосы	219
Узкополосный Сигнал и Расширение Спектра	220
Интерференция Многолучевого Распространения	222
Расширение Спектра Скачкообразной Перестройкой Частоты	223
Перестроечная последовательность	225
Время передачи	225
Время перестройки	225
Модуляция	226
Расширение Спектра Прямой последовательности	227
Кодирование Данных DSSS	227
Модуляция	228
Спектральная Мaska Передачи	230
Мультиплексирование с Ортогональным Частотным Разделением	231
Сверточное кодирование	232
Модуляция	233
Спектральная Мaska Передачи	235
Множественный доступ с ортогональным частотным разделением	237
Промышленные, Научные и Медицинские Полосы	238

Полоса ISM 900 МГц	238
Полоса ISM 2.4 ГГц	239
Полоса ISM 5.8 ГГц	239
Нелицензируемые 5 ГГц Полосы Национальной Информационной Инфраструктуры	240
U-NII-1	240
U-NII-2A	241
U-NII-2C	241
U-NII-3	242
U-NII-4	242
60 ГГц для Wi-Fi	243
Ниже 1 ГГц	244
Каналы 2.4 ГГц	244
Каналы 5 ГГц	247
Долгосрочная эволюция (LTE) в 5 ГГц	251
Каналы 6 ГГц	253
Существующее использование 6 ГГц	256
Автоматизированная Координация Частот	256
6 ГГц в Мире	257
Рассуждения о Wi-Fi в 6 ГГц	258
Итого	259
Темы Экзамена	260
Контрольные Вопросы	261
<b>Глава 7 Топологии Беспроводных ЛВС</b>	<b>265</b>
Топологии Беспроводных Сетей	267
Беспроводная Сеть Широкого Охвата	268
Беспроводная Городская Сеть	268
Беспроводная Персональная Сеть	269
Беспроводная Локальная Сеть	270
Станции 802.11	271
Станция-Клиент	272
Станция-Точка Доступа	272
Интеграционный Сервис	272
Система Распространения	273
Беспроводная Система Распространения	274
Составы Сервисов 802.11	276
Идентификатор Состава Сервиса	276
Базовый Состав Сервиса	277
Область Базового Сервиса	278
Идентификатор Базового Состава Сервиса	279
Несколько Идентификаторов Базового Состава Сервиса	280
Расширенный Состав Сервиса	282
Независимый Базовый Состав Сервиса	283
Персональный Базовый Состав Сервиса	285
Базовый Состав Сервиса с поддержкой Взаимосвязности	285
Базовый Состав Сервиса с поддержкой качества (QoS)	287

	Режимы настройки 802.11	288	
	Режимы Точки Доступа	288	
	Режимы Клиентской Станции	289	
	Итого	290	
	Темы Экзамена	290	
	Контрольные Вопросы	292	
<b>Глава</b>	<b>8</b>	<b>Доступ к Среде 802.11</b>	<b>297</b>
	CSMA/CA против CSMA/CD	298	
	Обнаружение Конфликтов	299	
	Функция Распределенной Координации	300	
	Физической Контроль Несущей	301	
	Виртуальной Контроль Несущей	302	
	Псевдослучайный Таймер Отсрочки	305	
	Межкадровое Пространство	307	
	Функция Гибридной Координации	308	
	Расширенный Распределенный Доступ к Каналу	309	
	Доступ к Каналу, Контролируемый Функцией	310	
	Гибридной Координации		
	Wi-Fi Мультимедиа	310	
	Справедливость Эфирного Времени	313	
	Итого	316	
	Темы Экзамена	316	
	Контрольные Вопросы	317	
<b>Глава</b>	<b>9</b>	<b>802.11 MAC</b>	<b>321</b>
	Пакеты, Кадры и Биты	323	
	Канальный уровень	324	
	Блок Сервисных Данных MAC	324	
	Блок Данных Протокола MAC	324	
	Физический Уровень	325	
	Блок Сервисных Данных PLCP	325	
	Блок Данных Протокола PLCP	326	
	Совместимость 802.11 и 802.3	326	
	802.11 MAC Заголовок	327	
	Контрольное Поле Кадра	328	
	Поле Длительности/ID	331	
	Адресация MAC Уровня	331	
	Поле Контроля Последовательности	339	
	Поле Контроля Качества (QoS)	340	
	Поле Контроля Высокой Пропускной Способности (HT)	340	
	Тело Кадра 802.11	341	
	Окончание 802.11	341	
	Машина Состояний 802.11	343	
	Кадры Управления	344	
	Маяк	344	
	Аутентификация	351	

	Ассоциация	352
	Переассоциация	356
	Деассоциация	358
	Деаутентификация	358
	Кадр Действия	358
	Кадры Контроля	361
	Кадр Подтверждения (ACK)	361
	Блоковое Подтверждение	364
	PS-Poll	365
	RTS/CTS	365
	CTS-to-Self	367
	Механизмы Защиты	367
	Кадры Данных	370
	Кадры Данных QoS и Non-QoS	371
	Кадры, Не Переносящие Данные	372
	Управление Электропитанием	373
	Устаревшее Управление Питанием	374
	Энергосбережение WMM PS и U-APSD	377
	Управление Питанием в MIMO	379
	Управление Питанием в 802.11ax	379
	Итого	380
	Темы Экзамена	380
	Контрольные Вопросы	382
<b>Глава 10</b>	<b>Технология MIMO: HT и VHT</b>	<b>387</b>
	MIMO	391
	Радиотехнические Цепи	393
	Пространственное Мультиплексирование	394
	Сравнение разнесений MIMO и SISO	397
	Комбинация Максимального Отношения	398
	Пространственно-Временное Блочное Кодирование	399
	Разнесение Циклического Сдвига	400
	Формирование Луча по Передаче	400
	Явное Формирование Луча	402
	Многопользовательское MIMO	404
	Многопользовательское Формирование Луча	406
	Каналы	409
	Каналы 20 МГц	409
	Каналы 40 МГц	410
	Сорокамегагерцевая нетолерантность	412
	Каналы 80 МГц и 160 МГц	413
	Зашитный Интервал	415
	Модуляция 256-QAM	417
	802.11n/ac PPDUs	422
	Non-HT	422
	Смешанный HT [HT Mixed]	422

VHT	423
802.11n/ac MAC	424
A-MSDU	424
A-MPDU	426
Блоковое Подтверждение	427
Управление Питанием	427
Модуляция и Схема Кодирования	429
Скорости Передачи Данных 802.11ac	432
Механизмы Защиты в HT/VHT	434
Режимы Защиты НТ (0–3)	434
Сертификация Wi-Fi Альянса	435
Итого	438
Темы Экзамена	438
Контрольные Вопросы	440
<b>Глава 11 Архитектура БЛВС</b>	<b>445</b>
Клиентские Устройства БЛВС	447
Форм Факторы Радиомодулей 802.11	448
Чипсеты Радиомодулей 802.11	455
Клиентские Утилиты	455
Плоскости Управления, Контроля и Данных	458
Плоскость Управления	459
Плоскость Контроля	459
Плоскость Данных	460
Архитектура БЛВС	460
Архитектура Автономной БЛВС	461
Централизованная Система Управления Сетью	463
Архитектура Централизованной БЛВС	465
Архитектура Распределенной БЛВС	473
Архитектура Гибридной БЛВС	475
Специальная Инфраструктура БЛВС	476
Маршрутизаторы БЛВС Филиалов Предприятий	476
Взаимосвязанные Точки Доступа БЛВС	477
Мосты БЛВС	478
Системы Позиционирования Реального Времени	481
VoWiFi	482
Облачные Сети	484
Программируемый Интерфейс Приложений	488
Транспорт и Форматы Данных	488
БЛВС APIs	490
Типовые Приложения	490
Управление Инфраструктурой	491
Протоколы Управления	492
Итого	497
Темы Экзамена	498
Контрольные Вопросы	499

<b>Глава</b>	<b>12</b>	<b>Питание по Ethernet (PoE)</b>	<b>503</b>
		История PoE	504
		Нестандартное PoE	505
		IEEE 802.3af	505
		IEEE Std 802.3-2005, Статья 33	505
		IEEE 802.3at-2009	505
		IEEE Std 802.3-2018, Статья 33	506
		IEEE 802.3bt-2018	506
		Устройства с PoE	507
		Питаемое Устройства	507
		Оборудование Подачи Питания	509
		Конечное Оборудование Подачи Питания	510
		Промежуточное Оборудование Подачи Питания	516
		Планирование и Разворачивание PoE	524
		Планирование Мощности	524
		Резервирование (Избыточность)	527
		Понижение Возможностей PoE	528
		Доводы о Мощности 802.3bt	528
		Итого	530
		Темы Экзамена	531
		Контрольные Вопросы	532
<b>Глава</b>	<b>13</b>	<b>Концепции Проектирования БЛВС</b>	<b>537</b>
		Проектирование Покрытия БЛВС	539
		Принятый Сигнал	540
		Отношение Сигнал-Шум	541
		Динамическое Переключение Скоростей	543
		Мощность Передачи	544
		Проектирование Роуминга	546
		Первичное и Вторичное Покрытие	549
		Быстрый Безопасный Роуминг	550
		Роуминг Уровня 3	551
		Проектирование Каналов	553
		Интерференция Смежных Каналов	553
		Переиспользование Каналов 2.4 ГГц	554
		Одноканальная Интерференция	557
		Переиспользование Каналов 5 ГГц	560
		Каналы DFS	562
		Проектирование Каналов 40 МГц	568
		Статические Каналы и Мощность Передачи или Адаптивное Радио	570
		Одноканальная Архитектура	572
		Проектирование Емкости	576
		Высокая Плотность	577
		Управление Выбором Полосы	582
		Балансировка Нагрузки	585

	Потребление Эфирного Времени	586
	Голос по сравнению с Данными	590
	Два 5 ГГц Радиомодуля и Программно-Определяемый Радиомодуль	593
	Проектирование БЛВС в 6 ГГц	596
	Обзор Клиентов	597
	Обзор Покрытия	598
	Переиспользование 6 ГГц Каналов	598
	Обнаружение ТД 6 ГГц	599
	Безопасность Wi-Fi в 6 ГГц	602
	Физическая Среда	603
	Антенны	604
	Наружное Проектирование	609
	Итого	610
	Темы Экзамена	611
	Контрольные Вопросы	613
<b>Глава 14</b>	<b>Обследование и Контрольное Обследование</b>	<b>617</b>
	Интервью об Обследовании Места БЛВС и о Проекте	620
	Брифинг с Заказчиком	621
	Бизнес Требования	621
	Требования по Емкости и Покрытию	623
	Существующая Беспроводная Сеть	625
	Обновление Существующей БЛВС	626
	Подключение к Инфраструктуре	627
	Ожидания по Безопасности	629
	Гостевой Доступ	630
	Эстетика	631
	Обследование вне Помещений	631
	Обзор Вертикальных Рынков	632
	Правительство	633
	Образование	633
	Здравоохранение	633
	Розница	634
	Склады и Производства	634
	Многоофисные Здания	635
	Устаревшее Обследование ТД-на-Палке	635
	Анализ Спектра	636
	Анализ Покрытия	640
	Гибридное Обследование	646
	Первичное Посещение	646
	Предиктивный Дизайн	648
	Контрольное Обследование	650
	Емкость и Пропускная Способность	652
	Роуминг	653

Задержка и Джиттер	654
Связь	654
Эстетика	654
Инструменты Обследования	655
Инструменты Обследования Внутри Помещений	655
Инструменты Обследования Вне Помещений	658
Документы и Отчеты	661
Бланки и Документация Заказчика	661
Предоставляемые результаты	663
Дополнительные Отчеты	664
Итого	665
Темы Экзамена	667
Контрольные Вопросы	668
<b>Глава 15 Решение Проблем БЛВС</b>	<b>673</b>
Пять Принципов Решения Проблем БЛВС	675
Передовой Опыт Решения Проблем	675
Решение Проблем по Модели OSI	677
Большинство Проблем являются Проблемами с Клиентом	679
Надлежащий Проект БЛВС Уменьшает Количество Проблем	680
БЛВС Всегда Виноват	681
Решение Проблем Уровня 1	681
Проект БЛВС	681
Мощность Передачи	682
Радиоинтерференция	683
Драйверы	687
PoE	688
Ошибки в Прошивке	688
Решение Проблем Уровня 2	689
Повторные Передачи Уровня 2	689
Радиоинтерференция	693
Низкий SNR	693
Интерференция Смежных Каналов	694
Скрытый Узел	695
Несовпадающая Мощность	700
Многолучевой Распространение	702
Решение Проблем Безопасности	702
Решение Проблем с PSK	703
Решение Проблем с 802.1X/EAP	705
Решение Проблем с VPN	713
Решение Проблем Роуминга	715
Утилизация Канала	719
Решение Проблем Уровней 3-7	721
Инструменты Решения Проблем БЛВС	725
Приложения по Обнаружению БЛВС	725
Анализаторы Спектра	726

	Анализаторы Протоколов	727
	Инструмент Проверки Пропускной Способности	729
	Стандартные Команды Проверки IP Сети	731
	Безопасная Оболочка [Secure Shell]	732
	Итого	733
	Темы Экзамена	733
	Контрольные Вопросы	734
<b>Глава 16</b>	<b>Беспроводные Атаки, Вторжение и Политика</b>	<b>741</b>
	Беспроводные Атаки	742
	Неучтенные Беспроводные Устройства	743
	Атаки Равный-Равный	747
	Прослушивание	749
	Взлом Шифрования	753
	Атака с Переустановкой Ключа [KRACK Attack]	754
	Уязвимость Kr00k	754
	Аутентификационные Атаки	755
	Подмена MAC	757
	Использование Уязвимостей Интерфейса	
	Управления	757
	Беспроводной Угон [Hijacking]	758
	Атаки Отказа-в-Обслуживании (DoS)	759
	Атаки на Оборудование Конкретного Производителя	762
	Социальная Инженерия	763
	Мониторинг Вторжения	763
	Система Предотвращения Беспроводного Вторжения	763
	Обнаружение Неучтенной ТД и Уменьшение Ее	767
	Влияния	
	Анализаторы Спектра	770
	Политики Беспроводной Безопасности	771
	Общие Политики Безопасности	771
	Рабочие Политики Безопасности	772
	Соответствие Законодательству	772
	Рекомендации по Политикам Беспроводной Безопасности в 802.11	774
	Итого	776
	Темы Экзамена	777
	Контрольные Вопросы	778
<b>Глава 17</b>	<b>Архитектура Сетевой Безопасности 802.11</b>	<b>783</b>
	Основы Безопасности 802.11	785
	Конфиденциальность и Целостность Данных	786
	Аутентификация, Авторизация, и Учет (AAA)	788
	Сегментация	788
	Мониторинг и Политика	789
	Устаревшая Безопасность 802.11	789
	Устаревшая Аутентификация	790
	Статическое Шифрование WEP	791

	МАС Фильтры	796	
	Сокрытие SSID	796	
	Надежная Безопасность	798	
	Надежная Защищенная Сеть	799	
	Аутентификация и Авторизация	800	
	Аутентификация PSK	800	
	Проприетарная Аутентификация PSK	803	
	Одновременная Аутентификация Равных	805	
	Структура 802.1X/EAP	809	
	Типы EAP	812	
	Динамическая Генерация Ключей Шифрования	814	
	4-х Стороннее Рукопожатие	815	
	Шифрование БЛВС	817	
	Шифрование TKIP	818	
	Шифрование CCMP	819	
	Шифрование GCMP	820	
	Защита Кадров Управления	821	
	WPA2	821	
	WPA3	822	
	WPA3-Personal	822	
	WPA3-Enterprise	823	
	Улучшенная Открытость	825	
	Безопасность Wi-Fi 6 ГГц	827	
	Сегментация Трафика	827	
	VLANs	828	
	RBAC	830	
	Беспроводная Безопасность VPN	831	
	Просто о VPN	832	
	VPNы Зого Уровня	833	
	SSL VPNs	833	
	Установка VPN	833	
	Итого	835	
	Темы Экзамена	836	
	Контрольные Вопросы	837	
<b>Глава</b>	<b>18</b>	<b>Приноси Свое Собственное Устройство (BYOD) и Гостевой Доступ</b>	<b>841</b>
		Управление Мобильными Устройствами	844
		Устройства Компании против Персональных Устройств	845
		Архитектура MDM	846
		Регистрация в системе MDM	848
		Профили MDM	853
		Программный Агент MDM	855
		Управление через Эфир	856
		Управление Приложениями	858
		Самостоятельная Регистрация Устройств Сотрудниками	860
		Регистрация с Двумя SSID	862

	Регистрация с Одним SSID	862	
	MDM или Самостоятельная Регистрация	863	
	Доступ в Гостевую БЛВС	864	
	Гостевой SSID	864	
	Гостевой VLAN	866	
	Гостевые Политики Межсетевого Экрана	867	
	Перехватывающие Веб Порталы	868	
	Изоляция Клиентов, Ограничение Скорости, и Фильтрация Содержимого Веб	871	
	Управление Гостевым Доступом	873	
	Самостоятельная Регистрация Гостей	874	
	Поручительство Сотрудников	876	
	Логин Социальной Сети	877	
	Шифрованный Гостевой Доступ	878	
	Хотспот 2.0 и Пасспоинт	879	
	Протокол Опроса Сетей Доступа	879	
	Архитектура Хотспот 2.0	881	
	802.1X/EAP и Хотспот 2.0	882	
	Онлайн Регистрация	883	
	Роуминговые Соглашения	885	
	Контроль Сетевого Доступа	885	
	Состояние устройства	886	
	Отпечаток ОС	887	
	AAA	890	
	Изменение Авторизации (CoA) по RADIUS	891	
	Единый Вход [Single Sign-On]	892	
	Итого	894	
	Темы Экзамена	895	
	Контрольные Вопросы	897	
<b>Глава</b>	<b>19</b>	<b>802.11ax: Высокая Эффективность</b>	<b>901</b>
	802.11ax = Wi-Fi 6	903	
	Перегруженность Wi-Fi Трафика	904	
	Обзор Высокой Эффективности	906	
	Многопользовательский	907	
	OFDMA	908	
	Поднесущие	909	
	Ресурсные Блоки	910	
	Триггерные Кадры	914	
	OFDMA в Нисходящем Канале	917	
	OFDMA в Восходящем Канале	918	
	Отчеты Состояния Буфера	919	
	Индикация Режима Работы	921	
	MU-MIMO	922	
	Цвет BSS и Пространственное Переиспользование	926	
	OBSS	926	
	Цвет BSS	929	

	Работа Пространственного Переиспользования	930	
	Целевое Время Пробуждения	933	
	Дополнительные Возможности 802.11ax PHY и MAC	934	
	1024-QAM	934	
	Длинное Символьное Время и Защитные Интервалы	935	
	Заголовки PHY 802.11ax	936	
	Только 20 МГц	938	
	AMPDU с Множеством Идентификаторов Трафика	939	
	Ключевые Вопросы Wi-Fi 6	939	
	Клиенты	939	
	Мультигигабитный Ethernet	940	
	Питание по Ethernet	942	
	4×4:4 или 8×8:8	943	
	80 МГц и 160 МГц Каналы	944	
	СЕРТИФИЦИРОВАННЫЙ Wi-Fi 6	945	
	Итого	946	
	Контрольные Вопросы	947	
<b>Глава</b>	<b>20</b>	<b>Установка БЛВС и Вертикальные Рынки</b>	<b>951</b>
	Рекомендации по Разворачиванию Типовых		
	Поддерживаемых БЛВС Приложений и Устройств	953	
	Данные	953	
	Голос	954	
	Видео	954	
	Сервисы Определения Местоположения Реального		
	Времени	955	
	Технология Зоны Непосредственной Близости iBeacon	955	
	Мобильные Устройства	958	
	Доступ к Корпоративным Данным и Мобильность	958	
	Конечных Пользователей		
	Расширение Сети на Удаленные Области	959	
	Мосты: Соединение Здание-Здание	960	
	Беспроводной ISP: Последняя Мил Для Передачи Данных	961	
	Небольшой Офис/Домашний Офис	961	
	Временная Офисная Сеть	962	
	Офисы Филиалов	963	
	Wi-Fi Удаленного Работника	963	
	Применение в Образовании/Классах	964	
	Промышленность: Склады и Производство	965	
	Розница	965	
	Здравоохранение	967	
	Муниципальные Сети	968	
	Хотспоты: Сети С Публичным Доступом	968	
	Сети Стадионов	970	
	Сети на Транспорте	970	
	Сети Правоохранительных Органов	971	
	Сети Служб Экстренного Реагирования	972	
	Провайдеры Услуг по Управлению	973	

Конвергенция Фиксированной и Мобильной Связи	973
БЛВС и Здоровье	974
Интернет Вещей	974
Производители БЛВС	975
Итого	977
Темы Экзамена	977
Контрольные Вопросы	978
<b>Приложение А Ответы на Контрольные Вопросы</b>	<b>983</b>
Глава 1: Обзор Беспроводных Стандартов, Организаций и Основ	984
Глава 2: Стандарт и Поправки IEEE 802.11	985
Глава 3: Основы Радиотехники	988
Глава 4: Радио Компоненты, Меры, и Математика	990
Глава 5: Радиосигнал и Основы Теории Антенн	992
Глава 6: Беспроводные Сети и Технологии Расширения Спектра	994
Глава 7: Топологии Беспроводных ЛВС	996
Глава 8: Доступ к Среде 802.11	999
Глава 9: 802.11 MAC	1002
Глава 10: Технология MIMO: HT и VHT	1005
Глава 11: Архитектура БЛВС	1007
Глава 12: Питание по Ethernet (PoE)	1010
Глава 13: Концепции Проектирования БЛВС	1013
Глава 14: Обследование и Контрольное Обследование	1017
Глава 15: Решение Проблем БЛВС	1019
Глава 16: Беспроводные Атаки, Вторжение и Политика	1022
Глава 17: Архитектура Сетевой Безопасности 802.11	1025
Глава 18: Приноси Свое Собственное Устройство (BYOD)	1028
Глава 19: 802.11ax: Высокая Эффективность	1031
Глава 20: Установка БЛВС и Вертикальные Рынки	1034
<b>Приложение В Аббревиатуры и Акронимы</b>	<b>1037</b>
Сертификации	1037
Организации и Регуляторы	1038
Меры	1039
Технические Термины	1040
<i>Указатель</i>	1101

# Таблица Упражнений

<b>упражнение</b>	<b>3.1</b>	Визуальная Демонстрация Поглощения . . . . .	104
<b>упражнение</b>	<b>3.2</b>	Визуальная Демонстрация Многолучевого Распространения и Фазы . . . . .	111
<b>упражнение</b>	<b>4.1</b>	Пошаговое Использование Правила 10-ти и 3-х. . . . .	138
<b>упражнение</b>	<b>4.2</b>	Пример Правила 10-ти и 3-х . . . . .	139
<b>упражнение</b>	<b>4.3</b>	Бюджет Линии Связи и Запас на Замирание . . . . .	155
<b>упражнение</b>	<b>9.1</b>	Просмотр Кадров-Маяков . . . . .	346
<b>упражнение</b>	<b>9.2</b>	Осмысление Зондирующих Запросов и Ответов. . . . .	350
<b>упражнение</b>	<b>9.3</b>	Использование Аутентификации Открытой Системы . . . . .	352
<b>упражнение</b>	<b>9.4</b>	Понимание Ассоциации. . . . .	353
<b>упражнение</b>	<b>9.5</b>	Понимание Переассоциации. . . . .	357
<b>упражнение</b>	<b>9.6</b>	Обзор Кадров Действия. . . . .	359
<b>упражнение</b>	<b>9.7</b>	Понимание Подтверждения . . . . .	362
<b>упражнение</b>	<b>9.8</b>	Использование Кадров Данных . . . . .	373
<b>упражнение</b>	<b>14.1</b>	Вычисление Затухания(Потерь) в Кабеле. . . . .	660
<b>упражнение</b>	<b>17.1</b>	Использование Нешифрованных и Зашифрованных Кадров Данных . . . . .	787
<b>упражнение</b>	<b>17.2</b>	SAE и Процесс 4x-Стороннего Рукопожатия . . . . .	808
<b>упражнение</b>	<b>17.3</b>	Процесс 802.1X/EAP и 4x-Стороннего Рукопожатия . . . . .	816



# Предисловие

Wi-Fi это одна из самых широко принятых технологий в мире. Сегодня, почти каждое мобильное устройство поставляется с Wi-Fi. Согласно компании Интернэшнл Дата Корпорэйшн [International Data Corporation], установленная база составляет свыше 13 миллиардов Wi-Fi устройств, и это количество продолжает расти, с более чем 4,5 миллиарда Wi-Fi устройств, прогнозируемым к поставке ежегодно в 2024 году, согласно исследованиям АБИ Рисеч [ABI Research].

Повсеместность Wi-Fi гарантировалась не всегда. Когда первый протокол 802.11 был выпущен в 1997 году, не было организаций по стандартам чтобы гарантировать, что продукты разных производителей могли бы продуктивно работать вместе. Так, в 1999 году, когда первоначальный стандарт Wi-Fi был представлен вместе с 802.11b, был образован Wi-Fi Альянс в качестве глобальной организации, чтобы обеспечить мультивендорную совместимость для продуктов беспроводных сетей, которая гарантирует лучшую работу и с более надежным соединением. СЕРТИФИЦИРОВАННЫЙ Wi-Fi [Wi-Fi CERTIFIED] был основан, чтобы обозначить продукты, которые удовлетворяют требованиям Wi-Fi Альянса по совместной работе, и устройства с отличительным логотипом Wi-Fi с тех пор стали синонимами высокого качества и надежности.

Программы СЕРТИФИЦИРОВАННЫЙ Wi-Fi [Wi-Fi CERTIFIED] значительно способствовали быстрому росту Wi-Fi, и сегодня СЕРТИФИЦИРОВАННЫЙ Wi-Fi [Wi-Fi CERTIFIED] международная признанная печать подтверждения с более чем 50 000 сертификация. Устройства подвергаются безжалостным испытаниям, обеспечивая гарантию того, что широкий диапазон Wi-Fi устройств будет работать совместно. Логотип СЕРТИФИЦИРОВАННЫЙ Wi-Fi [Wi-Fi CERTIFIED] теперь появляется на продуктах по всему миру, указывая на соответствие совместимости, безопасности и простоты использования стандартов.

Wi-Fi Альянс старается идти дальше чем совместимость, и содействует некоторым областям, которые позволяют Wi-Fi стать одной из наиболее знакомой и повсеместно используемой технологией. Безопасность, универсальность и простота использования были ключевыми целевыми областями. Wi-Fi Альянс создал Защищенный Доступ по Wi-Fi [Wi-Fi Protected Access] как основанную на стандартах, совместимую архитектуру безопасности для обеспечения чтобы обеспечить беспрецедентный уровень безопасности на всех СЕРТИФИЦИРОВАННЫХ Wi-Fi устройствах, и продолжила развивать стандарты безопасности, представив недавно СЕРТИФИЦИРОВАННЫЙ Wi-Fi WPA3. В дополнение к гарантированию того, что Wi-Fi остается безопасным, СЕРТИФИЦИРОВАННЫЙ Wi-Fi позволяет отрасли беспроводной связи подключать расширяющийся список потребительских электронных устройств, от мобильных телефонов и 4K ультра HD телевизоров до домашних терmostатов и дверных звонков, помогая разрабатывать программы , которые улучшают производительность устройств в разных средах, при этом понижая потребление электроэнергии для некоторых приложений. Наконец, Wi-Fi Альянс сделал технологию Wi-Fi доступной широкой публике, представив такие программы, как СЕРТИФИЦИРОВАННЫЙ Wi-Fi Легкий Контакт [Wi-Fi CERTIFIED EasyConnect], который делает конфигурирование Wi-Fi устройства столь простым, как сканирование QR кода продукта.

Хотя прошлое Wi-Fi впечатляющие, возможности технологии только продолжают расти. В начале 2020 года Федеральная Комиссия по Связи США [ U.S. Federal Communication Commission (FCC) ] приняла историческое решение - открыть нелицензируемый спектр в 6ГГц полосе для использования Wi-Fi. Вскоре после этого, Британский Департамент Связи [UK Office of Communications (Ofcom)] анонсировал, что будет освобождать часть спектра

в диапазоне 6Гц для использования Wi-Fi внутри помещений. В тоже время, регуляторы по всему миру также обсуждают использование 6Гц полосы в своих странах для нелицензируемого спектра. С 6 ГГц полосой, фактически, ресурсы спектра становятся доступными для увеличения экономического вклада Wi-Fi, давая дорогу более быстрым, с большей емкостью и с меньшей задержкой Wi-Fi устройствам и сетям.

Чтобы гарантировать совместимость и стимулировать дальнейший рост Wi-Fi, Wi-Fi Альянс расширил СЕРТИФИЦИРОВАННЫЙ Wi-Fi 6 [Wi-Fi CERTIFIED 6] на 6 ГГц—в характеристиках Wi-Fi 6E—так, что пользователи могут быстро получить выгоду от этой дополнительной емкости.

Будущее выглядит ярким и для технологии и для профессионалов, которые нашли свое призвание на этом динамичном и ставящем вызовы поле. Всегда есть что-то новое, чтобы узнать, новые головоломки, которые нужно решить. Я надеюсь, что эта книга пробудит ваш интерес к этим возможностям впереди, и с вышней сертификацией CWNA у вас на руках, вы сможете уверенно начать карьеру, которая несомненно будет вознаграждена и персонально и профессионально.

Марк Хунг [Mark Hung]

Вице Президент по Технологиям и Инжинирингу

Wi-Fi Альянс

Декабрь 2020 года

# Введение

Если вы приобрели эту книгу или думаете о приобретении этой книги, то вероятно у вас есть определенный интерес в сдаче сертификационного экзамена Сертифицированный Администратор Беспроводных Сетей CWNA® (Certified Wireless Network Administrator), или в узнать побольше о том, что содержит сертификационный экзамен CWNA. Мы хотели бы поздравить Вас с этим первым шагом, и мы надеемся, что наша книга сможет помочь Вам на вашем пути. Беспроводные сети являются одной из ажиотажных технологий на рынке. Также как со многими быстро растущими технологиями, спрос на знающих людей часто выше, чем предложение. Сертификация CWNA – это один из способов доказать, что у вас есть знания и навыки, чтобы поддержать эту растущую отрасль. Это Учебное Пособие было написано с этой целью. Эта книга была написана, чтобы помочь научить Вас беспроводным сетям так, чтобы у Вас были знания не только сдать сертификационный экзамен CWNA, но и проектировать, устанавливать и поддерживать беспроводные сети. Сертификация CWNA является обязательным предварительным требованием для учебных курсов, предлагаемых многими основными производителями БЛВС. В конце каждой главы мы включили контрольные вопросы, чтобы помочь Вам проверить Ваши знания и подготовиться к тестированию. Мы также включили упражнения и учебную онлайн среду для дальнейшего оснащения вашего обучения.

Прежде чем мы расскажем вам о процессе сертификации и требованиях, мы должны упомянуть, что эта информация может измениться ко времени сдачи вашего экзамена. Мы рекомендуем вам посетить [www.cwnp.com](http://www.cwnp.com), когда вы будете готовиться к тестированию, чтобы определить, какие текущие темы и требования.



Не заучивайте вопросы и ответы! Контрольные вопросы в этой книге разработаны, чтобы проверить ваши знания концепции или темы, которые скорее всего будут на экзамене CWNA. Контрольные вопросы будут отличаться от реальных вопросов сертификационного экзамена. Если вы изучаете и понимаете темы и задачи, то вы будете лучше подготовлены к тесту.

## О CWNA® и CWNP®

Если вы когда-либо готовились к сдаче сертификационного экзамена по технологии, с которой вы не знакомы, то вы знаете, что занимаетесь не только, чтобы изучить другую технологию, но также вероятно узнать об отрасли, с которой вы не знакомы. Читайте далее и мы расскажем Вам о CWNP.

CWNP это сокращение от *Certified Wireless Network Professional*, что в переводе означает Сертифицированный Профессионал Беспроводных Сетей. Экзамена CWNP нет. Программа CWNP разрабатывает учебные материалы и сертификационные экзамены для технологий беспроводных ЛВС в отрасли вычислительных сетей. Сертификационная программа CWNP – это нейтральная к производителю программа. Программа CWNP предлагает восемь сертификаций с фокусом на Wi-Fi и беспроводную технологию 802.11. Недавно, программа CWNP также начала предлагать сертификационный трек по другим беспроводным технологиям с фокусом на подключении Интернета Вещей [Internet of Things (IoT)].

Цель CWNP сертифицировать людей по беспроводным сетям, а не по продуктам определенного производителя. Да, временами авторы этой книги и создатели сертификации будут говорить, демонстрировать или даже учить как использовать определенный продукт; однако, цель в общем понимании беспроводной связи, а не самого по себе продукта. Если вы учились водить автомобиль, вы должны были физически садиться и практиковаться на нем. Когда вы подумаете об этом и вспомните, вы вряд ли скажете, что вы учились водить Форд; вы, вероятно, скажете, что вы учились водить на Форде.

Программа CWNP предлагает следующие восемь сертификаций по Wi-Fi:

**CWS: Certified Wireless Specialist [Сертифицированный Специалист по Беспроводным Сетям]** CWS это сертификационный экзамен по БЛВС (CWS- 100) начального уровня для тех кто в продажах, маркетинге и на начальных позициях, связанных с Wi-Fi. CWS обучает языку Wi-Fi и является прекрасным введением в Wi-Fi уровня предприятий.



**CWT: Certified Wireless Technician [Сертифицированный Технический Специалист по Беспроводным Сетям]** CWT – это сертификационный экзамен по БЛВС (CWT-100) начального уровня для обучения техников установке и настройке Wi-Fi на базовом уровне. CWT дает навыки, необходимые для установки и настройки ТД согласно спецификации и настройке клиентского устройства для подключения к и использования БЛВС.



**CWNA: Certified Wireless Network Administrator [Сертифицированный Администратор Беспроводных Сетей]** Сертификация CWNA – это сертификационный экзамен (CWNA-108) уровня администрирования Wi-Fi для сетевиков, которые находятся в поле, и которым необходимо тщательное понимание поведения радиоволн, обследования, установки и базовой корпоративной безопасности Wi-Fi. CWNA – это где вы узнаете как радио и IP соединяются вместе в Wi-Fi сеть. Сертификация CWNA была первоначальной сертификацией программы CWNP, и считалась сертификацией базового уровня в Wi-Fi отрасли. CWNA – это базовая сертификация для Wi-Fi уровня предприятия в семействе сертификаций CWNP и трамплином к получению сертификаций CWSP, CWDP, CWAP, и CWNE.



**CWSP: Certified Wireless Security Professional [Сертифицированный Профессионал по Беспроводной Безопасности]** Сертификационный экзамен CWSP (CWSP-206) это Wi-Fi сертификация профессионального уровня для сетевых инженеров, кто заинтересован в организации своей экспертизы в безопасности корпоративного Wi-Fi. В противоположность популярному мнению, корпоративный Wi-Fi может быть безопасен, если ИТ профессионалы устанавливают и настраивают его с пониманием того, как защитить беспроводную сеть. Вы должны иметь действующий CWNA, чтобы пройти экзамен CWSP.



**CWDP: Certified Wireless Design Professional [Сертифицированный Профессионал по Проектированию Беспроводных Сетей]** Сертификационный экзамен CWDP (CWDP-303) – это карьерная сертификация профессионального уровня для сетевиков, кто уже сертифицирован на CWNA, и обладает полным пониманием радиотехнологий и приложений сетей 802.11. Курс обучения CWDP готовит профессионалов БЛВС для надлежащего проектирования беспроводных ЛВС для оптимальной работы разных приложений в разных обстановках. Вы должны иметь действующий CWNA для прохождения экзамена CWDP.



**CWAP: Certified Wireless Analysis Professional [Сертифицированный Профессионал по Анализу Беспроводных Сетей]** Сертификационный экзамен CWAP (CWAP-403) – это карьерная сертификация профессионального уровня для сетевиков, кто уже сертифицирован на CWNA, и обладает полным пониманием радиотехнологий и приложений сетей 802.11. Курс обучения CWAP готовит профессионалов БЛВС анализировать, устранять проблемы, и оптимизировать любые беспроводные ЛВС. Вы должны иметь действующий CWNA, чтобы пройти экзамен CWAP.



**CWNE: Certified Wireless Network Expert [Сертифицированный Эксперт по Беспроводным Сетям]** Сертификация CWNE является сертификацией высшего уровня в программе CWNP. При успешном выполнении требований CWNE, вы продемонстрируете, что вы обладаете наиболее продвинутыми навыками, доступными на сегодняшний день на рынке беспроводных ЛВС. Сертификация CWNE требует сертификаций CWNA, CWAP, CWDP, и CWNP. Начиная с 1 января 2021 года, все кандидаты на CWNE должны обладать сертификацией CWISA и одной внешней сетевой сертификацией. Чтобы получить сертификацию CWNE, должно быть отправлено подробная анкета-заявление и она должна быть одобрена Советом Консультантов CWNE.

Требуется как минимум три года подтверждаемого, задокументированного, постоянного профессионального рабочего опыта, связанного с корпоративными сетями Wi-Fi. Кандидаты CWNE также должны отправить три рецензии от людей, знакомых с историей работы с корпоративным Wi-Fi сетями кандидата.



**CWNT: Certified Wireless Network Trainer [Сертифицированный Тренер по Беспроводным Сетям]** Сертифицированные Тренеры по Беспроводным Сетям - это квалифицированные инструкторы, сертифицированные по программе CWNP, для проведения учебных курсов CWNP для IT профессионалов. CWNTs - это технические эксперты и эксперты по преподаванию по беспроводным технологиям, продуктам и решениям. Чтобы гарантировать лучшее качество обучения, CWNP Партнера по Обучению [CWNP Education Partners] требуют использовать CWNT для проведения тренингов по официальным курсам CWNP. Больше информации о том, как стать CWNT доступно на вебсайте CWNP.



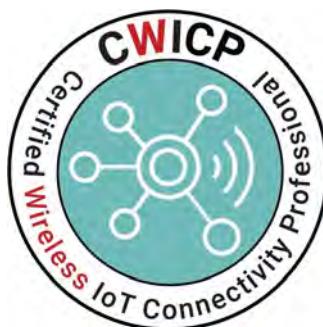
Кроме того, программа CWNP предлагает три сертификации с особым фокусом на беспроводных IoT технологиях:

**CWISA: Certified Wireless IoT Solutions Administrator [Сертифицированный Администратор по Беспроводным Решениям IoT]** Сертификация CWISA была разработана из-за того, что многие профессионалы БЛВС призывались для администрирования не-802.11 беспроводных решений в дополнение к Wi-Fi. Этот экзамен покрывает знания базового уровня по Bluetooth Низкого Энергопотребления [Bluetooth Low Energy (BLE)], Zigbee, беспроводных сервисов определения местоположения, и сотовых решений.

Кандидаты на экзамен также проверяются на знания на высоком уровне об API и концепции сетевой автоматизации.



**CWICP: Certified Wireless IoT Connectivity Professional [Сертифицированный Профессионал по Подключению Беспроводного IoT]** Сертификация CWICP требует умения работы с подключениями IoT и работы в промышленных и коммерческих сетях. Эти знания могут быть применены к развертыванию и решению проблем с наиболее распространенными протоколами беспроводного IoT с глубоким пониманием их работы. Эта сертификация особенно акцентирована на протоколах IEEE 802.15.4.



**CWIIP: Certified Wireless IoT Integration Professional [Сертифицированный Профессионал по Интеграции Беспроводного IoT]** Сертификация CWIIP является сертификацией продвинутого уровня, которая требуется для разработки систем с помощью API, программирования и библиотек. Необходимы фундаментальные навыки программирования на Python. Также требуется понимание протоколов беспроводного IoT таких, как MQTT, CoAP, DDS, и AMQP.



## Как Стать CWNA

Чтобы стать CWNA, вы должны сделать следующие две вещи: согласиться с тем, что вы прочитали и будете следовать правилам и условиям Соглашения о Конфиденциальности CWNP [CWNP Confidentiality Agreement], и пройти сертификационное испытание CWNA.



Копию Соглашения о Конфиденциальности CWNP [CWNP Confidentiality Agreement] можно найти на веб сайте CWNP.

Когда вы сядете сдавать экзамен, от вас потребуют принять это соглашение о конфиденциальности, прежде чем вы сможете продолжить тест. После того как вы согласились, вы сможете продолжить тест. Если вы пройдете тест, то тогда вы CWNA.

Информация об экзамене:

**Наименование экзамена:** Wireless LAN Administrator

**Номер экзамена:** CWNA-108

**Стоимость:** \$225 (в долларах США)

**Длительность:** 90 минут

**Вопросов:** 60

**Проходной порог:** 70 процентов (80 процентов для инструкторов)

**Доступные языки:** Английский

**Доступность:** Зарегистрироваться на Pearson VUE ([www.vue.com/cwnp](http://www.vue.com/cwnp))

Когда вы запишитесь на экзамен, вы получите инструкции, касательно процедуры выбора времени и отмены, требования к документам, удостоверяющим личность, и информацию о местоположении центра тестирования. Дополнительно вы получите письмо о подтверждении регистрации и платеже. Экзамен можно запланировать за неделю, или в некоторых случаях даже в тот же день. Вoucher на экзамен можно также приобрести на вебсайте CWNP.

После того, как вы успешно сдадите экзамен CWNA, программа CWNP наградит Вас сертификатом, который действителен три года. Для ресертификации вам нужно сдать действующий экзамен CWNA, CWSP, CWDP или CWAP, который действует на то время. Если информация, которую вы предоставили в центр тестирования верна, то вы получите электронное письмо от CWNP с признанием ваших достижений и предоставлением Вам сертификационный номер CWNP.



Мы настойчиво призываем вас перепроверить сайты CWNP и Pearson Vue за последними примерами политик и часто задаваемых вопросов (FAQ), когда вы начнете изучать CWNA, когда вы зарегистрируетесь на экзамен, и снова в дни перед экзаменом, так что бы вы были в курсе любых новых опций и изменений, или требований для сдающих экзамены.

## Кому Стоит Купить Эту Книгу?

Если вы хотите иметь твердый фундамент в беспроводных сетях, и ваша цель подготовиться к экзамену - эта книга для Вас. Вы найдете ясное объяснение концепций, которые вы должны уяснить, и много помохи, чтобы достичь высокого уровня профессиональной компетентности, который вам нужен для успеха.

Если вы хотите стать сертифицированным CWNA - эта книга определенно то, что вам нужно. Однако, если вы всего лишь хотите попытаться сдать экзамен без реального понимания беспроводных технологий, это Учебное пособие не для Вас. Оно написано для людей, которые хотят приобрести реальный опыт и глубокие знания по беспроводным сетям. Профессионалы по БЛВС по всему миру покупают эту книгу в качестве справочного руководства по технологии 802.11. Эта книга считается лучшим нейтральным к производителю справочным руководством по Wi-Fi для Администраторов ИТ.

## Как Использовать Эту Книгу и Онлайн Ресурсы

Мы включили несколько проверочных функций в книгу и онлайн ресурсы. Эти инструменты помогут Вам запомнить жизненно важное содержание экзамена, а также подготовить Вас к реальному экзамену.

**Прежде Чем Вы Начнете** В начале книги (сразу после этого введения) есть оценочный тест, который вы можете использовать, чтобы проверить вашу готовность к экзамену. Пройдите этот тест прежде, чем вы начнете читать книгу; это поможет Вам определить области, в которых Вам может понадобиться навести порядок. Ответы на оценочный тест показаны на отдельной странице после последнего вопроса теста. Каждый ответ включает объяснение и замечание, указывающее Вам главу, в которой представлен материал.

**Контрольные Вопросы в Каждой Главе** Чтобы проверять ваши знания по мере освоения книги, есть контрольные вопросы в конце каждой Главы. Когда вы закончили Главу, ответьте на контрольные вопросы и затем проверьте ваши ответы. Вы можете вернуться и перечитать раздел, который касается каждого вопроса, на который вы ответили неправильно, чтобы гарантировать, что вы ответите правильно в следующий раз, когда будете проверяться на знание материала.

## Учебная Онлайн Среда Sybex

Учебная Онлайн Среда Sybex для этой книги включает карточки для запоминания [flashcards], симулятор экзамена, и словарь. Чтобы начать использовать это для подготовки к экзамену CWNA, зайдите на [www.wiley.com/go/sybextestprep](http://www.wiley.com/go/sybextestprep), зарегистрируйте вашу книгу, чтобы получить Ваш уникальный ПИН код, вернитесь на [www.wiley.com/go/sybextestprep](http://www.wiley.com/go/sybextestprep) и зарегистрируйте новую учетную запись или добавьте эту книгу к существующей учетной записи. Это применимо только к книгам на английском языке.

**Симулятор Экзамена** Симулятор экзамена [test engine] содержит два бонусных практических экзамена. Вы можете использовать их, как если бы вы проходили экзамен, для того чтобы оценить вашу готовность. Симулятор экзамена также содержит все контрольные вопросы, содержащиеся в конце глав, и оценочные вопросы из начала книги. Вы можете выбрать вопросы из определенной Главы или вы можете запустить симулятор с

перемешанными вопросами из нескольких Глав или бонусных экзаменов. Симулятор экзамена может быть в режиме практики [practice mode] (где вы можете видеть подсказки), а также в режиме экзамена (как настоящий экзамен). Также применим только для английской версии книги.

**Карточки для Запоминания [Flashcards]** Это короткие вопросы и ответы, как те, которые вы вероятно использовали в школе, но эти карточки – онлайн. Применимо для английской версии книги.

**Словарь** Этот словарь – это электронный список ключевых терминов и их определений.

## Дополнительные Онлайн Ресурсы

**Упражнения** Несколько Глав в этой книге содержат лабораторные работы, которые используют ресурсы, которые вы можете загрузить с сайта книги ([www.wiley.com/go/cwnasgbe](http://www.wiley.com/go/cwnasgbe)). Эти упражнения дают вам более широкий учебный опыт путем предоставления практики и пошагового решения проблем. Некоторые из включенных материалов, которые вы можете загрузить включают перехваченные PCAP кадры, чтобы закрепить то, что вы узнали о беспроводных кадрах 802.11 в Главах 9 “802.11 MAC”, и 17, “Архитектура Сетевой Безопасности 802.11.”

**Информационные бюллетени [White Papers]** Несколько Глав в этой книге ссылаются на информационные бюллетени «белые страницы» о беспроводных сетях, которые доступны на соответствующих вебсайтах. Эти информационные листы служат дополнительным справочным материалом при подготовке к экзамену CWNA.

### Получение Помощи Онлайн

Мы надеемся, что ваш опыт с Учебной Онлайн Средой Sybex и дополнительными онлайн ресурсами будет без шероховатостей. Но, если у вас возникнут какие-либо проблемы с онлайн материалами или самой книгой, пожалуйста, сообщите о вашей проблеме нашей команде круглосуточной технической поддержке по адресу [support.wiley.com](mailto:support.wiley.com). У них есть живой онлайн чат и вариант общения по электронной почте. Применимо для английской версии книги.

## Цели Экзамена CWNA (CWNA-108)

Экзамен CWNA измеряет ваше понимание основ поведения радиоволн, вашей способности описать характеристики и функции компонентов беспроводной ЛВС, и ваши знания о навыках, необходимых для установки, настройки и решения проблем периферийного оборудования беспроводной ЛВС и протоколов.

Навыки и знания, измеряемые этим экзаменом, были получены из обследования экспертов и профессионалов по беспроводным сетям. Результаты этого обследования были использованы для расставления весов предметным областям, и гарантирования того, что расstawление весов отражает относительную важность содержания.

Следующая таблица приводит разбивку экзамена, показывающую вес каждого раздела:

Предметная Область	% Экзамена
Радиотехнологии	15%
Регулирование и стандарты БЛВС	20%
Протоколы и устройства БЛВС	20%
Сетевая архитектура и концепции проектирования БЛВС	15%
Сетевая безопасность БЛВС	10%
Подтверждение радиохарактеристик	10%
Решение проблем БЛВС	10%
<b>Итого</b>	<b>100%</b>

## **Радиотехнологии – 15%**

### **1.1 Определить и объяснить базовые характеристики радиоволн и поведение радиоволн.**

- Длина волны, частота, амплитуда, фаза, синусоидальные волны
- Распространение радиоволн и покрытие
- Отражение, рефракция, дифракция, и рассеяние
- Многолучевое распространение и радиointерференция
- Усиление и затухание
- Усиление
- Аттенюация
- Поглощение
- Коэффициент Стоячей Волны по Напряжению (KCBH)
- Обратные потери
- Затухание на пути в свободном пространстве (FSPL)

### **1.2 Применять базовые концепции радиоматематики и единицы измерения**

- Ватт и милливатт
- Децибел (дБ)
- дБм и дБи
- Уровень шума

- SNR
- RSSI
- Правила 10 и 3 преобразования дБм в мВт
- Эквивалентная изотропно излучаемая мощность (ЭИИМ)

### **1.3 Определять характеристики радиосигнала по отношению к антеннам**

- Радиосигнал и физическая линия прямой видимости и чистота зоны Френеля
- Ширина луча
- Пассивное усиление
- Поляризация
- Типы антенного разнесения
- Радиотехнические цепи
- Пространственное мультиплексирование
- Формирование луча передачи (TxBF)
- Комбинация максимальных отношений (MRC)
- MIMO

### **1.4 Объяснять и применять функциональность радиоантенн и антенных систем и доступных аксессуаров**

- Всенаправленные антенны
- Полунаправленные антенны
- Узконаправленные антенны
- Ориентация антенны
- Читать Азимутальные и вертикальные диаграммы различных типов антенн
- Радиочастотные кабели и разъемы
- Грозозащитники и заземляющие стержни/проводы

## **Регулирование и Стандарты БЛВС – 20%**

### **2.1 Объяснить роли организаций сетевой и БЛВС отраслей**

- IEEE
- Wi-Fi Альянс
- IETF
- Области регулирования и организации

**2.2 Объяснять и применять различные решения Физического Уровня (PHY) IEEE стандарта 802.11-2016 а также поправок, включая поддерживаемые ширины каналов, пространственные потоки, и скорости передачи данных**

- DSSS – 802.11
- HR-DSSS – 802.11b
- OFDM – 802.11a
- ERP – 802.11g
- Wi-Fi 4 – HT – 802.11n
- Wi-Fi 5 – VHT – 802.11ac
- Wi-Fi 6 – HE – 802.11ax

**2.3 Понимать технологии расширения спектра, Модуляцию, и Схемы Кодирования (MCS)**

- DSSS
- OFDM
- OFDMA и ресурсные блоки
- BPSK
- QPSK
- QAM (16, 24, 256, 1024)

**2.4 Определять и применять функциональные концепции БЛВС 802.11**

- Первичные каналы
- Смежные перекрывающиеся и не перекрывающиеся каналы
- Пропускная способность против скорости передачи данных
- Ширина полосы пропускания
- Защитный интервал

**2.5 Описать уровни модели OSI, затрагивающие стандарт 802.11-2016 и поправки**

**2.6 Определять и соответствовать требованиям и ограничениям местного регулятора (особенно в 2.4 ГГц и 5 ГГц)**

- Полосы частот, используемые Физическим уровнем (PHY) 802.11
- Доступные каналы
- Регуляторные ограничения мощности
- Динамический выбор частоты (DFS)
- Контроль мощности передачи (TPC)

**2.7 Объяснить сценарии базового применения беспроводных сетей 802.11**

- Беспроводная ЛВС (БЛВС) – BSS и ESS
- Беспроводной мост
- Беспроводная сеть «на лету» (IBSS)
- Беспроводная взаимосвязь

**Протоколы и Устройства БЛВС – 20%****3.1 Опишите компоненты, которые составляют беспроводной состав сервиса 802.11**

- Станции (STAs)
- Базовый Состав Сервиса (BSS) (инфраструктурный режим)
- SSID
- BSSID
- Расширенный состав сервиса(ESS)
- IBSS ( «на лету» или Ad hoc)
- Система распространения (DS)
- Среда системы распространения (DSM)

**3.2 Определять терминологию, связанную с 802.11 MAC и PHY**

- MSDU, MPDU, PSDU, и PPDU
- A-MSDU и A-MPDU
- Преамбула и заголовок PHY

**3.3 Идентифицировать и объяснять формат кадра MAC**

- Формат кадра MAC
- Адресация кадра MAC

**3.4 Определять и объяснять назначение трех главных типов кадров 802.11**

- Кадры управления
- Кадры контроля
- Кадры данных

**3.5 Объяснять процесс нахождения и подключения к БЛВС**

- Сканирование (активное и пассивное)
- Аутентификация
- Ассоциация
- Открытая Система и Аутентификация с Общим Ключом

- Подключение к сетям с аутентификацией 802.1X/EAP и Предварительным общим ключом
- Выбор BSS
- Подключение к скрытым SSID

### **3.6 Объяснять методы доступа к каналам 802.11**

- DCF
- EDCA
- RTS/CTS
- CTS-to-Self
- NAV
- Межкадровые пространства (SIFS, DIFS, EIFS,AIFS)
- Обнаружение физической несущей и обнаружение виртуальной несущей
- Скрытый узел

### **3.7 Объяснить работу 802.11 MAC**

- Роуминг
- Режимы сбережения энергии и буфферизация кадров
- Механизмы защиты

### **3.8 Описать характеристики, выбрать и установить устройства БЛВС, контроля, и системы управления.**

- Точки Доступа (ТД)
- Контроллеры БЛВС
- Системы управления беспроводных сетей
- Беспроводной мост и взаимосвязываемые ТД
- Клиентские устройства

## **Сетевая Архитектура и Концепции Проектирования БЛВС – 15%**

### **4.1 Описать и внедрить Питание по Ethernet (PoE) 802.3af, 802.3at, 802.3bt**

- Оборудование Подачи Питания (PSE)
- Питаемые Устройства
- Промежуточное и конечное оборудование подачи питания
- Классы питания для определения разницы между оборудованием подачи питания (PSE) и Питаемым Устройством (PD)
- Бюджеты Мощности и плотность портов с питанием

**4.2 Определять и описывать различия, преимущества, и ограничения различных архитектур беспроводных ЛВС.**

- Централизованная пересылка данных
- Распределенная пересылка данных
- Плоскости Контроля, Управления и Данных
- Решения по масштабируемости и доступности
- Туннелирование, Качество (QoS) и VLANы

**4.3 Описать такие факторы, принимаемые во внимание при проектировании для типовых сценариев внедрения в беспроводных сетях, как требования по покрытию, вопросы роуминга, пропускной способности, емкости и безопасности.**

- Факторы, принимаемые во внимание, для проектирования передачи данных
- Факторы, принимаемые во внимание, для проектирования передачи голоса
- Факторы, принимаемые во внимание, для проектирования для передачи видео
- Факторы, принимаемые во внимание, для проектирования сервисов местоположения, включая Сервисы Местоположения Реального Времени [Real-Time Location Services (RTLS)]
- Факторы, принимаемые во внимание, для проектирования для высоко мобильных устройств (т.е. планшетов и смартфонов)
- Планирование емкости для сред высокой и очень высокой плотности
- Факторы, принимаемые во внимание, для проектирования гостевого доступа/BYOD
- Факторы, принимаемые во внимание, для проектирования для поддержки устаревших устройств 802.11

**4.4 Продемонстрировать знание о типовых proprietарных характеристиках в беспроводных сетях**

- Справедливость Эфирного Времени
- Управление Полосой
- Характеристики динамической мощности и управления каналом

**4.5 Определять и настраивать требуемые сетевые сервисы, поддерживающие беспроводную сеть**

- DHCP для клиентской адресации, адресация ТД, и/или обнаружение контроллера
- Протоколы синхронизации времени (т.е., NTP, SNTP)
- VLANы для сегментации
- Службы аутентификации (RADIUS, LDAP)
- Списки Контроля Доступа для сегментации
- Требования к емкости проводной сети

## Сетевая Безопасность БЛВС – 10%

### 5.1 Определять слабые опции безопасности, которые не следует использовать в корпоративных БЛВС

- WEP
- Аутентификация с Общим Ключом
- Сокрытие SSID как механизм безопасности
- Фильтрация по MAC
- Использование не рекомендуемых методов безопасности (например, WPA и/или WPA2 с TKIP)
- Защищенная Установка Wi-Fi (WPS)

### 5.2 Определять и настраивать эффективные механизмы защиты для корпоративных БЛВС

- Применение AES с CCMP для шифрования и целостности
- WPA2-Personal, включая ограничения и передовой опыт для использования заранее известного ключа (PSK)
- WPA2-Enterprise, настройка беспроводных сетей для использования 802.1X, включая подключение к серверам RADIUS и соответствующие методы EAP

### 5.3 Понимание базовых концепций WPA3 и Гибкой Беспроводной Безопасности (OWE) и улучшений по сравнению с WPA2

- Понимание улучшений базовой безопасности в WPA3 по сравнению с WPA2
- Понимать улучшения базовой безопасности шифрования и целостности WPA3 (например, CCMP, GCMP, AES)
- Одновременная Аутентификация Равных (SAE) в WPA3, как улучшение для устаревшей технологии с заранее известным общим ключом (PSK)
- Понимать назначение Гибкого Беспроводного Шифрования [Opportunistic Wireless Encryption (OWE)] для публичных и гостевых сетей

### 5.4 Описать типовые варианты безопасности и инструменты, используемые в беспроводных сетях

- Решения контроля доступа (например, перехватывающие порталы [captive portals], NAC, BYOD)
- Защищенные кадры управления
- Методы Быстрого Безопасного Роуминга
- Система Предотвращения Беспроводного Вторжения (WIPS и/или обнаружение неконтролируемой [rogue] ТД)
- Анализаторы протоколов и спектра
- Передовой опыт в безопасных протоколах управления (например, шифрованное управление через HTTPS, SNMPv3, SSH2, VPN, и управление паролями)

## Контрольное радиообследование – 10%

### 6.1 Подтверждать и предоставлять документы, что требования проекта выполнены, включая покрытие, пропускную способность, роуминг, и возможность подключения в контролльном обследовании после установки

### 6.2 Локализовать и определять источники радиоинтерференции

- Определять сбой в радиочасти от беспроводных устройств 802.11, включая борьбу или интерференцию и причины/источники обоих, включая одноканальную борьбу [co-channel contention (CCC)], перекрывающиеся каналы, и беспроводные устройства 802.11 зоны непосредственной близости
- Идентифицировать источники радиоинтерференции от не-802.11 беспроводных устройств, на основе исследования утилизации частоты и эфирного времени
- Понимать опции борьбы с интерференцией, включая устранение источника интерференции или изменение использования беспроводного канала

### 6.3 Производить тестирование приложений для подтверждения производительности БЛВС

- Тестирование сети и доступности сервисов
- Тестирование VoIP
- Тестирование приложения реального времени
- Тестирование пропускной способности

### 6.4 Понимать и использовать базовые характеристики инструментов подтверждения

- Использовать тестеры пропускной способности для задач подтверждения
- Использовать программное обеспечение для подтверждения беспроводной сети (особенно программы обследования и сканеры беспроводных сетей)
- Использовать анализаторы протоколов для задач подтверждения
- Использовать анализаторы спектра для задач подтверждения

## Решение проблем БЛВС – 10%

### 7.1 Описать и применять типовые инструменты решения проблем, используемых в БЛВС

- Использовать анализаторы протоколов для задач решения проблем
- Использовать анализаторы спектра для определения источников интерференции
- Использовать управление, мониторинг и системы журналирования (logging) для задач решения проблем
- Использовать сканнеры беспроводных ЛВС для задач решения проблем

### 7.2 Идентифицировать и решать типовые беспроводные проблемы

- Определять причины недостаточной пропускной способности в беспроводных системах распространения (WDS), включая неправильную настройку скорости/дуплекса порта LAN [LAN], недостаточности бюджета PoE, и недостаточности полосы в Интернет или WAN
- Определять и решать вопрос радиоинтерференцией с помощью анализатора спектра

## Терминология Экзамена CWNA

Программа CWNP использует специфичную терминологию, когда формулирует вопрос в любом экзамене CWNP. Используемая терминология наиболее часто отражает тот же самый язык, который используется Wi-Fi Альянсом и в IEEE. Хотя цели экзамена CWNA относятся к стандарту IEEE802.11-2016, последняя текущая версия IEEE стандарта 802.11 – это документ IEEE 802.11-2020, который включает все поправки, которые были приняты до публикации документа. Организации по стандартам, такие как IEEE, часто создают несколько поправок к стандарту до объединения принятых поправок (финализированных и утвержденных версий) в новый стандарт.



Чтобы надлежащим образом подготовиться к экзамену CWNA, каждый кандидат должен быть на 100 процентов знаком с терминологией, используемой программой CWNP. Эта книга определяет и охватывает всю терминологию, включая акронимы, термины и определения.

## Политика Использования Авторизованных Материалов CWNP

CWNP не прощает использование неразрешенных учебных материалов, также называемых “брейн дампс” [brain dumps – в переводе с английского - всеобъемлющая запись мыслей и идей. А фактически - это запись реальных вопросов реального экзамена и ответов на него]. Люди, которые используют такие материалы для сдачи экзамена CWNA будут лишены своих сертификаций. В попытке более ясно донести политику CWNP по использованию неразрешенных учебных материалов, CWNP направляет всех кандидатов на сертификацию на Политику Поведения Кандидата в CWNP [CWNP Candidate Conduct Policy], которая доступна на сайте CWNP. Пожалуйста прочитайте эту политику до начала процесса обучения по любому экзамену CWNP. От кандидатов в начале экзамена потребуют указать, что они понимают и следуют этой политике.

## Советы по Сдаче Экзамена CWNA

Несколько общих советов как успешно сдать экзамен:

- Возьмите с собой два вида удостоверений личности. Одно должно быть с фотографией, например, водительские права. Другое может быть основной кредитной картой или паспортом. Оба вида должны содержать вашу подпись.
- Приезжайте пораньше в центр тестирования так, чтобы вы смогли успокоиться и просмотреть ваши учебные материалы, особенно таблицы и списки с информацией, касающиеся экзамена.
- Читайте вопросы внимательно.
- Не поддавайтесь первому заключению. Убедитесь, что вы точно знаете, что спрашивается в вопросе.
- Будут вопросы с несколькими правильными ответами.
- Когда есть более одного правильного ответа, сообщение внизу экрана будет подсказывать вам или “выберите два” [“choose two”], или “выберите все, что применимо” [“choose all that apply.”]. Обязательно читайте высвечиваемые сообщения, чтобы знать сколько правильных ответов вы должны выбрать.
- Когда отвечаете на вопросы с множественным выбором в которых вы не уверены, используйте процесс исключения, чтобы убрать очевидно неправильный ответ в первую очередь. Поступая так, вы улучшите ваши шансы, если вам нужно сделать обдуманный выбор.

- Не тратьте слишком много времени на один вопрос.
- Этот тест с выбором ответов; однако, вы не можете вернуться назад во время экзамена. Вы должны ответить на текущий вопрос прежде, чем вы сможете перейти к следующему вопросу, а после вы должны перейти к следующему вопросу, вы не можете вернуться назад и изменить ваш ответ на предыдущий вопрос.
- Следите за временем.
- Так как этот 90 минутный тест состоит из 60 вопросов, у вас будет в среднем 90 секунд, чтобы ответить на каждый вопрос. Вы можете потратить больше или меньше времени на каждый вопрос, но, когда пройдут 90 минут, тест завершится. Следите за вашим прогрессом. После 45 минут у вас должны быть даны ответы хотя бы на 30 вопросов. Если нет, не паникуйте. Вам просто нужно отвечать на оставшиеся вопросы побыстрее. Если в среднем вы сможете отвечать на оставшиеся 30 вопросов на 4 секунды быстрее, вы отыграете 2 минуты. И снова – не паникуйте; просто успокойтесь.
- Чтобы узнать последнюю стоимость экзамена и обновления в процедуре регистрации, посетите вебсайт CWNP по адресу [www.cwnp.com](http://www.cwnp.com).

# Оценочный Тест

1. На каком уровне модели OSI работает технология 802.11? (Выберите все, что применимо.)
  - A. Канальном [Data-Link]
  - B. Сетевом [Network]
  - C. Физическом [Physical]
  - D. Презентационном [Presentation]
  - E. Транспортном [Transport]
2. Какая сертификация Wi-Fi Альянса определяет механизм сбережения жизни аккумулятора, которое критично для ручных устройств таких, как сканер штрих кодов и VoWiFi телефонов?
  - A. WPA2-Enterprise
  - B. WPA2-Personal
  - C. WMM-PS
  - D. WMM-SA
  - E. Voice Enterprise
3. Какая из этих частот имеет самую большую длину волн?
  - A. 750 кГц
  - B. 2.4 ГГц
  - C. 252 ГГц
  - D. 2.4 МГц
4. Какой из этих терминов лучше подходит для сравнения взаимоотношения между двумя радиоволнами, которые делят между собой одну и ту же частоту?
  - A. Многолучевое распространение [Multipath]
  - B. Мультиплексирование [Multiplexing]
  - C. Фаза [Phase]
  - D. Расширение спектра [Spread spectrum]
5. Беспроводной мост передает на 10 мВт. Кабель вносит затухание в 3 дБ, а антенна дает усиление в 20 дБи. Чему равен ЭИИМ [EIRP]?
  - A. 25 мВт
  - B. 27 мВт
  - C. 4 мВт
  - D. 1 300 мВт
  - E. 500 мВт

- 6.** дБи – это выражение какого типа измерений?
- A.** Усиление точки доступа
  - B.** Принятая мощность
  - C.** Переданная мощность
  - D.** Усиление антенны
  - E.** Фактический выход
- 7.** Что из следующего является возможным эффектом Коэффициента Стоячей Волны по Напряжению (KCBN)? (Выберите все, что применимо.)
- A.** Увеличенная амплитуда
  - B.** Уменьшенная амплитуда
  - C.** Неисправность передатчика
  - D.** Непредсказуемая амплитуда
  - E.** Сигналы не в фазе
- 8.** При установке всенаправленной антенны с высоким усилением, что из следующего произойдет? (Выберите два.)
- A.** Увеличиться горизонтальное покрытие.
  - B.** Уменьшиться горизонтальное покрытие.
  - C.** Увеличиться вертикальное покрытие.
  - D.** Уменьшиться вертикальное покрытие.
- 9.** Радиомодули 802.11ac VHT обратно совместимы с какими радиомодулями IEEE 802.11? (Выберите два)
- A.** 802.11 устаревшие (FHSS) радиомодули
  - B.** 802.11g (ERP) радиомодули
  - C.** 802.11 устаревшие (DSSS) радиомодули
  - D.** 802.11b (HR-DSSS) радиомодули
  - E.** 802.11a (OFDM) радиомодули
  - F.** 2.4 ГГц 802.11n (HT) радиомодули
  - G.** 5 ГГц 802.11n (HT) радиомодули
- 10.** Какая поправка IEEE 802.11 определяет многопользовательскую работу в трех полосах частот?
- A.** IEEE 802.11n
  - B.** IEEE 802.11g
  - C.** IEEE 802.11ac
  - D.** IEEE 802.11ax
  - E.** IEEE 802.11w

- 11.** Какой из следующих параметров является разницей между мощностью основного радиосигнала и суммой радиоинтерференции и фонового шума?
- A.** Шумовое Отношение
  - B.** SNR
  - C.** SINR
  - D.** BER
  - E.** DFS
- 12.** Какие характеристики сигнала являются общими в расширении спектра и методах сигналов на основе OFDM? (Выберите два.)
- A.** Узкая ширина полосы
  - B.** Низкая мощность
  - C.** Высокая мощность
  - D.** Широкая ширина полосы
- 13.** Идентификатор состава сервиса [service set identifier] часто является синонимом чего из следующего?
- A.** Duration/ID
  - B.** ESSID
  - C.** BSSID
  - D.** PMKID
- 14.** Какой сценарий проекта ESS требуется стандартом IEEE 802.11-2020?
- A.** Две или более точек доступа с перекрывающимися зонами покрытия
  - B.** Две или более точек доступа с перекрывающимися несоединенными зонами покрытия
  - C.** Одна точка доступа с единой BSA
  - D.** Два базовых состава сервиса [basic service sets] соединенные средой системы распространения (DSM)
  - E.** Ничего из выше перечисленного
- 15.** Какие условия CSMA/CA должны быть выполнены прежде, чем радиомодуль 802.11 может передавать? (Выберите все, что применимо.)
- A.** Таймер NAV должен быть равен нулю.
  - B.** Случайный таймер обратного отсчета должен кончиться.
  - C.** ССА должен быть пустым.
  - D.** Должно быть надлежащее межкадровое пространство.
  - E.** Точка доступа должна быть в режиме PCF.
- 16.** Кадры управления типа маяк содержат какую из следующей информацию? (Выберите все, что применимо.)
- A.** Информацию о канале
  - B.** IP адрес назначения

- C. Базовые скорости передачи данных
  - D. Карта индикации трафика (TIM)
  - E. Проприетарную информацию производителя
  - F. Метку времени
17. Ребеку МакАдамс наняли для проведения анализа беспроводных пакетов вашей сети. Во время проведения анализа, она заметила, что многим кадрам данных предшествовал кадр RTS, за которым шел кадр CTS. Что могло бы быть причиной, чтобы это происходило? (Выберите все, что применимо.)
- A. ТД автоматически включает механизмы RTS/CTS как ответ на одноканальную интерференцию [co-channel interference].
  - B. ТД была настроена вручную с низкими порогами RTS/CTS.
  - C. Близко находящийся сотовый телефон является причиной того, что некоторые узлы включают защитный механизм.
  - D. Устаревшие клиенты 802.11b подключены к ТД 802.11g/n.
18. Какое другое название кадров данных 802.11, также называемых PSDU?
- A. PPDU
  - B. MSDU
  - C. MPDU
  - D. BPDU
19. Какое устройство БЛВС использует динамический и проприетарный протокол маршрутизации 2ого уровня?
- A. Коммутатор БЛВС [WLAN switch]
  - B. Контроллер БЛВС [WLAN controller]
  - C. Мршрутизатор БЛВС [WLAN router]
  - D. Взаимосоединяемая [Mesh] точка доступа БЛВС
20. Какой термин лучше всего описывает большой объем данных, генерируемых в Интернете, создаваемы сенсорами, датчиками, мониторами и машинами?
- A. Межмашинное взаимодействие [Machine-to-machine] (M2M)
  - B. Сети с поддержкой облаков [Cloud-enabled networking] (CEN)
  - C. Сети на основе облаков [Cloud-based networking ] (CBN)
  - D. Программное обеспечение как сервис [Software as a service] (SaaS)
  - E. Интернет вещей [Internet of Things] (IoT)
21. Какая технология делит канал, позволяя параллельным передачам небольших кадров нескольким пользователям происходить одновременно?
- A. OFDMA
  - B. OFDM
  - C. MU-MIMO
  - D. DSSS
  - E. HR-DSSS

- 22.** Какой термин лучше всего описывает как Wi-Fi может быть использован для определения поведения покупателя и покупательских тенденций?
- A.** Радио аналитика [Radio analytics]
  - B.** Аналитика заказчиков [Customer analytics]
  - C.** Розничная аналитика [Retail analytics]
  - D.** Аналитика местоположений [Location analytics]
- 23.** Проблема скрытого узла происходит, когда передачи одной клиентской станции не слышны некоторыми другими клиентскими станциями в зоне покрытия базового состава сервиса (BSS). Какие последствия проблемы скрытого узла? (Выберите все, что применимо.)
- A.** Повторные передачи
  - B.** Межсимвольная интерференция (ISI)
  - C.** Коллизии
  - D.** Увеличенная пропускная способность
  - E.** Уменьшенная пропускная способность
- 24.** Что является потенциальной причиной повторных передач на 2ом уровне? (Выберите все, что применимо.)
- A.** Радиоинтерференция
  - B.** Низкое отношение сигнал-шум (SNR)
  - C.** Двух частотные передачи
  - D.** Высокое отношение сигнал-шум (SNR)
  - E.** Одноканальная интерференция
- 25.** Какое из этих решений считается сильной безопасностью БЛВС?
- A.** Сокрытие SSID
  - B.** Фильтрация MAC
  - C.** WEP
  - D.** Аутентификация с Общим Ключом
  - E.** CCMP/AES
  - F.** TKIP
- 26.** Какой стандарт безопасности определяет контроль доступа на основе порта?
- A.** IEEE 802.11x
  - B.** IEEE 802.3bt
  - C.** IEEE 802.11i
  - D.** IEEE 802.1X
  - E.** IEEE 802.11s

- 27.** Что является лучшим инструментом по обнаружению радиопомехи при атаке отказа-в-обслуживании?
- A.** Программное обеспечение по анализу в области времени
  - B.** Анализатор протоколов
  - C.** Анализатор спектра
  - D.** Программное обеспечение по предиктивному моделированию
  - E.** Осциллограф
- 28.** Какая из этих атак может быть обнаружена системой предотвращения беспроводного вторжения (WIPS)? (Выберите все, что применимо.)
- A.** Подделка деаутентификации
  - B.** Подделка MAC
  - C.** Неконтролируемая (подставная) сеть «на-лету» (ad-hoc)
  - D.** Большой поток ассоциаций
  - E.** Неконтролируемая (подставная) ТД
- 29.** Вы были наняты Компанией XYZ, находящейся в США, для проведения радиообследования. Какое государственное агентство нужно проинформировать, прежде чем поставить башню, которая превышает 200 футов над уровнем земли? (Выберите все, что применимо.)
- A.** Организацию, регулирующую радио
  - B.** Местный муниципалитет
  - C.** Пожарный департамент
  - D.** Налоговую службу
  - E.** Авиационную службу
- 30.** Вы были наняты Корпорацией АБВ для проведения обследования внутри помещения. Какая информация будет в финальном отчете об обследовании? (Выберите два.)
- A.** Анализ Безопасности
  - B.** Анализ Покрытия
  - C.** Анализ Спектра
  - D.** Анализ Маршрутизации
  - E.** Анализ Коммутации
- 31.** Название потенциального источника радиоинтерференции в 5ГГц в U-NII полосе.
- A.** Беспроводной телефон
  - B.** AM радиостанция
  - C.** FM радиостанция
  - D.** Микроволновые печи
  - E.** Bluetooth

- 32.** Когда клиенты Wi-Fi 6E зайдут на рынок, какой предсказывается наиболее вероятный метод обнаружения ТД?
- A.** Активное сканирование 6 ГГц каналов с помощью кадров зондирующего запроса.
  - B.** Пассивное сканирование 6 ГГц каналов с помощью кадров-маяков.
  - C.** Внеполосное обнаружение с помощью уменьшенных отчетов о соседях (RNRs)
  - D.** Внутриполосное обнаружение с помощью уменьшенных отчетов о соседях (RNRs)
  - E.** Внутриполосное обнаружение с помощью кадров оповещения обнаружения Быстрой Начальной Установки Канала [Fast Initial Link Setup (FILS)]
- 33.** Что является причиной номер один повторных передач 2ого уровня?
- A.** Низкий SNR
  - B.** Скрытый узел
  - C.** Интерференция смежных зон
  - D.** Радиоинтерференция
- 34.** Что должно делать питаемое устройство (PD), чтобы считаться PoE совместимым (IEEE 802.3-2015, Статья 33)? (Выберите все, что применимо.)
- A.** Быть способным принимать питание в каждом из двух способов (через линию данных или неиспользуемые пары).
  - B.** Отвечать классификационной сигнатурой.
  - C.** Отвечать 35и-омной сигнатурой обнаружения.
  - D.** Отвечать 25и-омной сигнатурой обнаружения.
  - E.** Принимать 30 ватт мощности от оборудования подачи питания.
- 35.** Радиомодули Wi-Fi, использующие технологию 802.11n (HT), могут работать в каких полосах частот? (Выберите все, что применимо.)
- A.** 902–928 МГц
  - B.** 2.4–2.4835 ГГц
  - C.** 5.15–5.25 ГГц
  - D.** 5.47–5.725 ГГц
  - E.** 5.925–6.425 ГГц
- 36.** Какие методы используются для уменьшения служебной информации [overhead] MAC уровня, в соответствии с поправкой 802.11n-2009? (Выберите все, что применимо.)
- A.** A-MSDU
  - B.** A-MPDU
  - C.** MCS
  - D.** PPDU
  - E.** MSDU

- 37.** Артема попросили дать рекомендации о том, как предоставить Wi-Fi доступ корпоративным сотрудникам и устройствам в среде с высокой плотностью пользователей. Какая из этих стратегий проектирования БЛВС считается лучшей практикой? (Выберите все, что применимо.)
- A.** Для критически важных клиентских устройств, которые поддерживают полосы и 2,4 ГГц и 5 ГГц, создать SSID только для 5 ГГц.
  - B.** Для критически важных клиентских устройств, которые поддерживают полосы и 2,4 ГГц и 5 ГГц, создать SSID для обеих полос.
  - C.** Выключить 60 процентов или более 2,4 ГГц радиомодули на ТД.
  - D.** Выключить 60 процентов или более 5 ГГц радиомодулей на ТД.
  - E.** Не выключать никакие радиомодули ТД.
- 38.** Роя наняли для решения проблем в корпоративной Wi-Fi 6 сети. Заказчик недавно развернул двухчастотные 4×4:4, которые также включают в себя третий сенсорный радиомодуль для мониторинга WIPS. Большинство ТД работают в полной функциональности; однако, ТД в одном здании, кажется, что работают только как радиомодули 2×2:2, а сенсорный радиомодуль остановил свою работу. Что является наиболее вероятной основной причиной этой проблемы?
- A.** Проблема ТД – в том, что они подключены к портам коммутатора, которые поддерживают только 1Гбит каналы подключения.
  - B.** Проблема ТД в том, что они подключены к портам коммутатора, которые поддерживают только 802.3af (15.4 ватта).
  - C.** Проблема ТД в том, что они подключены коммутируемым портам доступа, а не к транковым 802.1Q портам.
  - D.** Проблема ТД в том, что они подключены к транковым коммутируемым 802.1Q портам и транковым портам доступа.
  - E.** Проблема ТД в том, что они подключены к полудуплексным коммутируемым портам.
- 39.** Что может быть доставлено через эфир на мобильные устройства БЛВС, такие как планшеты и смартфоны, когда развернуто решение по управлению мобильными устройствами (MDM)?
- A.** Конфигурационные настройки
  - B.** Приложения
  - C.** Сертификаты
  - D.** Веб закладки
  - E.** Все выше перечисленное
- 40.** Производители БЛВС начали предлагать возможность гостевым пользователям входить в гостевую БЛВС с уже существующей учетной записью в социальных сетях, таких как имя пользователя и пароль от Facebook или Twitter. Какая структура авторизации может быть использована для входа с помощью логинов социальных сетей в гостевые сети БЛВС?
- A.** Kerberos
  - B.** RADIUS
  - C.** 802.1X/EAP
  - D.** OAuth
  - E.** TACACS

# Ответы на Оценочный Тест

1. А и С. Стандарт IEEE 802.11-2020 определяет механизмы связи только на Физическом уровне и MAC подуровне Канального [Data-Link] уровня модели OSI. За дополнительной информацией обращайтесь к Главе 1.
2. С. WMM-PS помогает сохранить энергию аккумулятора для устройств, использующих Wi-Fi, путем управления временем, которое клиентские устройства проводят в спящем режиме. Сохранение срока жизни аккумуляторной батареи критично для таких ручных устройств, как сканер штрих кодов и VoWiFi телефонов. Чтобы использовать преимущества возможностей экономии энергии, и устройство и точка доступа должны поддерживать WMM- Power Save. За дополнительной информацией обращайтесь к Главе 8.
3. А. У сигнала 750 кГц примерная длина волны 1312 футов или 400 метров. У сигнала 252 ГГц примерная длина волны меньше чем 0,05 дюйма или 1,2 миллиметра. Помните, что чем выше частота сигнала, тем меньше длина волны соответствующего электромагнитного сигнала. За дополнительной информацией обращайтесь к Главе 3.
4. С. Фаза включает положение гребней и впадин амплитуды двух волновых форм. За дополнительной информацией обращайтесь к Главе 3.
5. Е. 10 мВт мощности уменьшено на 3 дБ, т.е. поделено на 2, получая 5 мВт. Это затем увеличено на 20 дБи, т.е. умножено на 10 дважды, давая 500 мВт. За дополнительной информацией обращайтесь к Главе 4.
6. Д. Теоретически, изотропный излучатель может излучать одинаковый сигнал во всех направлениях. Антенна не может делать это, из-за конструктивных ограничений. Однако, антенны часто сравниваются с изотропными излучателями потому, что они излучают радиоволновую энергию. Усиление, или увеличение мощности от антенны, при сравнении с тем, что изотропный излучатель сгенерировал бы, называется изотропные децибелы дБи. Еще один способ перефразирования – это увеличение децибелов по сравнению с изотропным излучателем, или изменение в мощности относительно антенны. дБи – это единица измерения усиления антенны. За дополнительной информацией обращайтесь к Главе 4.
7. В, С, и Д. Отраженное напряжение, вызванное несовпадением импедансов, может стать причиной деградации амплитуды, непредсказуемой силы сигнала, или в худшем случае даже выгорание передатчика. Смотрите Главу 5 для дополнительной информации.
8. А и Д. Когда усиление всенаправленной антенны увеличивается, то область вертикального покрытия уменьшается, в то время как горизонтальная область покрытия увеличивается. Смотрите Главу 5 для дополнительной информации.
9. Е и Г. Радиомодули 802.11ac (VHT) передают в полосах 5 ГГц U-NII и не совместимы с радиомодулями 2.4 ГГц, такими как 802.11 устаревшие (FHSS) радиомодули, 802.11 устаревшие (DSSS) радиомодули, 802.11b (HR-DSSS) радиомодули, 802.11g (ERP) радиомодули, или 802.11n радиомодули, которые передают в полосе частот ISM 2.4 ГГц. Радиомодули 802.11ac (VHT) обратно совместимы с 5 ГГц радиомодулями 802.11n (HT) и радиомодулями 802.11a (OFDM). За дополнительной информацией обращайтесь к Главе 6.

10. Д. Поправка 802.11ax определяет использование двух многопользовательских технологий: MU-MIMO и OFDMA. Эти многопользовательские технологии могут быть использованы в 2.4 ГГц, 5 ГГц, и 6 ГГц полосах частот. За дополнительной информацией обращайтесь к Главам 6 и 19.
11. С. Отношение сигнал к интерференции плюс шум (SINR) соотносит основной радиосигнал с интерференцией и шумом. В то время как уровень шума имеет тенденцию не сильно флюктуировать, интерференция от других устройств, вероятнее всего, будет типовой и частой. За дополнительной информацией обращайтесь к Главе 4.
12. В и D. Сигналы и расширения спектра и OFDM используют ширину полосы, которая шире, чем та, которая требуется для переноса данных и обладает меньшими требованиями к мощности передачи. Смотрите Главу 6 для дополнительной информации.
13. В. Наименование логической сети беспроводной ЛВС часто называется ESSID (идентификатор расширенного сервисного состава [extended service set identifier]) и, фактически, является синонимом SSID (идентификатором сервисного состава [service set identifier]), который является еще одним термином наименования логической сети в большинстве типовых установок БЛВС. За дополнительной информацией обращайтесь к Главе 7.
14. Е. Сценарии, описанные в вариантах А, В, С, и D, все являются примерами того, как расширенный состав сервиса может быть развернут. Стандарт IEEE 802.11-2020 определяет расширенный состав сервиса [extended service set (ESS)] как “набор из одного или более взаимосоединенных базовых составов сервиса”. Однако, стандарт IEEE 802.11-2020 не делает обязательным любой из примеров, приведенных в вариантах ответов. За дополнительной информацией обращайтесь к Главам 2 и 7.
15. А, В, С, и D. Множественный Доступ с Контролем Несущей и Предотвращением Конфликтов [Carrier Sense Multiple Access with Collision Avoidance] (CSMA/CA) - это метод доступа к беспроводной среде, который использует несколько проверок и балансов, чтобы попытаться минимизировать коллизии. Эти проверки и балансы можно также рассматривать как несколько линий обороны. Различные линии обороны установлены в надежде гарантировать, что только один радиомодуль передает, пока все остальные радиомодули слушают. Четыре линии обороны включают вектор занятия сети, случайный таймер отсрочки, оценку чистого канала, и межкадровое пространство. Для дополнительной информации обращайтесь к Главе 8.
16. А, С, D, Е, и F. Из списка выборов, единственная информация, которая не содержится в кадре управления типа маяк - это IP адрес назначения. Тело кадров управления 802.11 содержит только информацию уровня 2; следовательно, IP информация не включена в кадр. Другая информация, которая включена в маяк включает параметры безопасности и качества (QoS). Для дополнительной информации обращайтесь к Главе 9.

17. В и D. Радиомодули ТД могут быть настроены вручную для использования RTS/CTS для всех передач. Обычно это делается для диагностики проблем скрытого узла или для предотвращения проблемы скрытого узла, когда устанавливается беспроводной мост точка-многоточка. RTS/CTS автоматически включен как механизм защиты, когда устаревшие клиенты существуют в той же самой беспроводной среде, что и устройства с более новыми технологиями 802.11. Это обеспечивает обратную совместимость. За дополнительной информацией обращайтесь к Главе 9.
18. С. Техническое название кадра данных 802.11 - это блок данных протокола MAC [MAC protocol data unit] (MPDU). MPDU содержит заголовок уровня 2, тело кадра, и окончание, которое является 32х-битным CRC, которое называется как последовательность проверки кадра (FCS). Внутри тела кадра MPDU находится блок данных сервиса MAC [MAC service data unit] (MSDU), который содержит данные из LLC и уровней 3-7. Когда MPDUдвигается вниз к Физическому уровню, он называется PSDU. За дополнительной информацией обращайтесь к Главе 9.
19. D. Взаимосвязываемые [mesh] точки доступа БЛВС создают самоформирующуюся взаимосвязанную [mesh] сеть БЛВС, которая автоматически соединяет точки доступа во время установки и динамически обновляет маршруты по мере добавления клиентов. Большинство взаимосвязанных [mesh] сетей БЛВС используют проприетарные (собственные) протоколы маршрутизации 2ого уровня с такими параметрами, как RSSI, SNR, и клиентская нагрузка. За большей информацией обращайтесь к Главе 11.
20. Е. Годами, большая часть данных генерируемых в Интернете создавалась людьми. Теория Интернета Вещей [Internet of Things] (IoT) в том, что в будущем большая часть данных генерируемая в Интернете может создаваться сенсорами, датчиками и машинами. Радиомодуль 802.11 сетевых карт (NICs), используемых в качестве клиентских устройств стали появляться во множестве типов машин и устройств. За дополнительной информацией обращайтесь к Главе 11
21. А. Множественный доступ с Ортогональным множественным разделением [Orthogonal frequency-division multiple access] (OFDMA) - это технология, которая может быть найдена в радиомодулях Wi-Fi 6. Она позволяет 20 МГц каналам быть поделенными на девять небольших каналов, называемых ресурсными блоками (RUs), обеспечивающими многопользовательские передачи. За дополнительной информацией обратитесь к Главе 19.
22. С. Для дальнейшей поддержки и понимания заказчиков и их поведений, устанавливаются продукты розничной аналитики [retail analytics] для мониторинга перемещения заказчиков и их поведения. Стратегически размещенные точки доступа или датчики слушают зондирующие кадры от смартфонов с включенным Wi-Fi. MAC адреса используются для идентификации каждого уникального устройства, а силы сигнала используется для мониторинга и отслеживания местоположения покупателя. Розничная аналитика может идентифицировать путь, который взял покупатель, пока идет по магазину, вместе с проведенным временем в разных местах в магазине. Эта информация может использоваться для идентификации покупательской модели и анализа эффективности дисплеев внутри магазина и рекламы. За дополнительной информацией обращайтесь к Главе 20.

- 23.** А, С, и Е. Станции, которые не могут слышать скрытый узел, могут передавать в то же самое время, что и передающий скрытый узел. Это приведет к непрерывным коллизиям в передаче в полудуплексной среде. Коллизии будут повреждать кадры, а они должны будут отправлены повторно. Каждый раз когда нужны повторные передачи, добавляется больше служебной информации [overhead] к среде, приводящей к уменьшению пропускной способности. Межсимвольная интерференция является результатом многолучевого распространения [multipath], а не проблемой скрытого узла. За дополнительной информацией обращайтесь к Главе 15.
- 24.** А и В. Повторные передачи на Уровне 2 могут быть вызваны многими разными переменными в среде БЛВС. Многолучевое распространение, радиоинтерференция, скрытые узлы, интерференция смежных зон(сот), и низкое отношение сигнал-шум, являются возможными причинами повторных передач 2ого уровня. За дополнительной информацией обращайтесь к Главе 15.
- 25.** Е. Хотя вы можете скрыть ваш SSID, чтобы спрятать идентификатор вашей беспроводной сети от "мамкиных хакеров" [script kiddies] и не-хакеров, нужно ясно понимать, что скрытие SSID никаким образом не является окончательным решением беспроводной безопасности. Из-за возможности подделки [spoofing] и из-за всей работы администратора фильтрация по MAC не считается надежным средством безопасности для беспроводных корпоративных сетей. Аутентификация с Общим Ключом и WEP являются устаревшими решениями по безопасности 802.11. CCMP/AES определен в качестве типа шифрования по умолчанию поправкой по безопасности IEEE 802.11i. Взлом шифра AES может занять время жизни солнца с помощью инструментов, доступных сегодня. Для большей информации обращайтесь к Главе 17.
- 26.** Д. Стандарт IEEE 802.1X это не специальный беспроводной стандарт, и часто ошибочно указывается как IEEE 802.11x. Стандарт IEEE 802.1X - это стандарт контроля доступа на основе портов. IEEE 802.1X предоставляет архитектуру авторизации, которая разрешает или не разрешает трафику пройти через порт, и следовательно, получить доступ к сетевым ресурсам. За дополнительной информацией обращайтесь к Главе 17.
- 27.** С. Единственный инструмент, который абсолютно определит интерферирующий сигнал - это анализатор спектра. Анализатор спектра - это инструмент области уровня 1, который может обнаружить радиосигнал в сканируемом диапазоне частот. Некоторые производители БЛВС предлагают анализаторы спектра низкого класса в качестве встроенных возможностей своих точек доступа. За дополнительной информацией обращайтесь к Главе 16.
- 28.** А, В, С, D, и Е. Система предотвращения вторжений в беспроводные сети 802.11 (WIPs) может быть способна мониторить 200 атак или больше. Могут быть обнаружены любые DoS атаки 2ого уровня, атаки подмены [spoofing] и большинство неконтролируемых (подставных) [rogue] устройств. За дополнительной информацией обращайтесь к Главе 16.

- 29.** А, В, и Е. В Соединенных Штатах, если какая-либо башня превышает 200 футов над уровнем земли, то вы должны связаться с FCC и с FAA, которые являются регулирующими организациями по связи и авиации, соответственно. В других странах есть похожие ограничения по высоте, и нужно связаться с соответствующими организациями регулирующие радио и организацией по авиации для уточнения подробностей. Местные муниципалитеты могут иметь строительные правила или ограничения по высоте, а может потребоваться разрешение. За дополнительной информацией обращайтесь к Главе 14.
- 30.** В и С. Финальный отчет об обследовании, называется как предоставляемые материалы [deliverable], будет содержать информацию по анализу спектра, определяющую потенциальные источники интерференции. Анализ покрытия также будет определять границы зоны радиопокрытия. Финальный отчет также содержит рекомендуемые места установки точек доступа, конфигурационные настройки, и ориентацию антенн. Планирование емкости считается обязательным при проектировании БЛВС; обнако, тестирование пропускной способности приложений часто является опциональным аналитическим отчетом, включенным в финальный отчет об обследовании. Анализ безопасности, коммутации, и маршрутизации не включается в отчет об обследовании. За дополнительной информацией обращайтесь к Главе 14.
- 31.** А. Некоторые беспроводные телефоны передают на 5 ГГц полосе U-NII-3, и являются потенциальным источником радиоинтерференции, устройства Bluetooth передают в частотном пространстве 2.4 ГГц. Радиостанции FM и AM передают в лицензируемых частотах. Для дополнительной информации обращайтесь к Главе 14.
- 32.** С. Так как существует так много каналов в полосе 6 ГГц, клиентское зондирование может занять значительное количество времени. На удивление, но ожидается, что внеполосное обнаружение будет наиболее широко использоваться, даже для клиентов Wi-Fi 6E, уже ассоциированных с радиомодулем 6 ГГц ТД. ТД Wi-Fi 6E будут использовать информационный элемент уменьшенного отчета о соседях [reduced neighbor report] (RNR), которые может включать информацию о соседних ТД. Для Wi-Fi 6E "соседняя ТД" в действительности это радиомодуль 6 ГГц, который расположен в той же ТД вместе с радиомодулями 2,4 ГГц и 5 ГГц. Клиенты Wi-Fi 6E узнают о доступном радиомодуле 6 ГГц из информации RNR или кадрах маяках, или в зондирующих ответных кадрах, отправленных радиомодулями 2,4 ГГц и 5 ГГц ТД. За дополнительной информацией обращайтесь в Главу 13.
- 33.** D. Все ответы являются возможными причинами повторных передач на 2ом уровне; однако, радиоинтерференция является главной причиной появления повторных передач кадров на 2ом уровне. Производительность БЛВС снижается, если коэффициент повторных передач превышает 10 процентов. За дополнительной информацией обращайтесь к Главе 15.

34. А и Д. Для питаемых устройств [powered device (PD)] таких как, точка доступа, чтобы считаться, что она совместима с IEEE 802.3-2015, Статья 33 стандарта PoE, устройство должно быть способно принимать питание по линиям для передачи данных или по неиспользуемым витым парам кабеля Ethernet. Питающее устройство (PD) должно также отвечать оборудованию подачи питания (PSE) 25и-омной сигнатурой определения. PD может ответить классификационной сигнатурой, но это является опциональным. Текущий стандарт PoE позволяет максимальное потребление в 12,95 ватт Питающим устройством (PD) от оборудования подачи питания. За дополнительной информацией обращайтесь к Главе 12.
35. В, С, и Д. Технология высокой пропускной способности [High throughput (HT)] определена поправкой IEEE 802.11n-2009 и не зависит от частоты. 802.11n (HT) может работать в полосе ISM 2,4 ГГц, так же как и во всех полосах U-NII 5 ГГц. Радиомодули 802.11n иногда называют названием поколения Wi-Fi 4. За дополнительной информацией обращайтесь к Главам 2 и 10.
36. А и В. Поправка 802.11n-2009 вводит два новых метода агрегации кадров, чтобы помочь уменьшить служебную информацию [overhead]. Агрегация кадров - это метод комбинации нескольких кадров в передачу одного кадра. Первый метод агрегации кадров называется как агрегированный блок данных сервиса MAC [aggregate MAC service data unit] (A-MSDU). Второй метод агрегации кадров называется как агрегированный блок данных протокола MAC [aggregate MAC protocol data unit] (A-MPDU). За дополнительной информацией обращайтесь к Главам 2 и 10.
37. А и С. На предприятиях полоса 2,4 ГГц часто считается "не гарантированной" [“best effort”] полосой частот, и 5 ГГц каналы резервируются для всех других клиентов, которые требуют параметры высокой производительности. Еще одна стратегия, которая иногда используется для разделения устройств по двум полосам частот - это SSID сегментация. Другими словами, критически важные SSID вещаются только в 5 ГГц полосе. В средах с высокой плотностью, часто 60-75 процентов радиомодулей 2,4 ГГц выключают, чтобы помочь минимизировать одноканальную интерференцию [co-channel interference]. За дополнительной информацией обращайтесь к Главе 13.
38. В. Производители корпоративных БЛВС встроили технологию понижения уровня PoW в свои ТД. Это позволяет ТД работать на низкой мощности, но за счет потери некоторой функциональности. Один из методов - понижение возможностей MIMO ТД. Например, производитель может также уменьшить число радиотехнических цепей в радиомодуле 4x4:4 до 2x2:2. Другие сетевые интерфейсы, такие как радиомодуль BLE, сенсорный радиомодуль Wi-Fi, или Ethernet порт также могут быть отключены, чтобы уменьшить потребляемую мощность. За дополнительной информацией обратитесь к Главе 12.
39. Е. Решение по управлению мобильными устройствами может использоваться и для устройств компании (CID) и для собственных устройств [bring your own device (BYOD)], который принадлежать сотрудникам. Решения MDM предлагают возможности установки и распространения через эфир сертификатов безопасности, веб закладок, приложений и конфигурационных настроек. За дополнительной информацией обратитесь к Главе 18.

- 40.** D. Авторизационная архитектура OAuth 2.0 позволяет сторонним приложениям получить ограниченный доступ к HTTP сервису и часто используется для логинов социальных сетей для гостевых Wi-Fi сетей. За дополнительной информацией обращайтесь к Главе 18.



# Глава 1

# Обзор Беспроводных Стандартов, Организаций и Основ

---

**В ЭТОЙ ГЛАВЕ ВЫ УЗНАЕТЕ О  
СЛЕДУЮЩЕМ:**

- ✓ История беспроводных локальных вычислительных сетей
- ✓ Организации по Стандартам
  - Федеральная Комиссия по Связи
  - Международный Союз Электросвязи  
Сектор Радиосвязи
  - Институт Инженеров по Электротехнике и Электронике
  - Подразделение Инженерных Задач Интернета
  - Wi-Fi Альянс
  - Международная Организация по Стандартизации
- ✓ Ядро, распределение и доступ
- ✓ Основы связи
  - Терминология связи
  - Несущие сигналы
  - Методы модуляции



Технология *Беспроводной Локальной Вычислительной Сети* (БЛВС) [Wireless local area network (WLAN)] имеет долгую историю, которая возвращает нас в 1970-е годы, с корнями, уходящими аж в 19ый век. Эта глава начнется с краткой истории технологии БЛВС. Изучение новой технологии может показаться пугающей задачей.

Так много новых акронимов, аббревиатур, сокращений, терминов и идей, с которыми нужно познакомится. Один из ключей для изучения любой темы - это изучение основ. Учтесь ли вы водить автомобиль, управлять самолетом, или устанавливать беспроводные сети, существуют базовые правила, принципы, и концепции, которые однажды изучив, обеспечивают вас "строительными блоками" для вашего дальнейшего обучения.

Технология Института Инженеров по Электротехнике и Электронике (IEEE) 802.11, обычно называемая Wi-Fi, является стандартной технологией для предоставления связи для локальной вычислительной сети (ЛВС) [local area network (LAN)] с использованием радиоволн [radio frequencies (RFs)]. IEEE называет стандарт 802.11-2020 как руководство для предоставления рабочих параметров для БЛВС. Многочисленные организации по стандартам и регулирующие организации помогают управлять и направлять беспроводные технологии и связанную с этим отрасль. Наличие некоторых знаний об этих различных организациях может снабдить вас пониманием того, как IEEE 802.11 работает, и иногда даже, как и почему стандарты развиваются тем путем, которым они развиваются.

По мере того, как вы становитесь более знающим о беспроводных сетях, вы можете захотеть, или вам может понадобится прочитать некоторые документы по стандартам, которые созданы различными организациями. Вместе с информацией об организациях по стандартам, эта глава включает краткий обзор их документов.

В дополнение к обзору различных организаций по стандартам, которые ведут и регулируют Wi-Fi, эта глава обсуждает где технология БЛВС[WLAN] соответствует базовым принципам сетевого проектирования. Наконец, эта глава дает обзор некоторых основ связи и модуляции данных, которые не являются частью экзамена CWNA, но могут помочь вам лучше понять беспроводную связь.

### Чем Отличается Акроним от Аббревиатуры?

В мире науки и технологии, обычное дело сокращать технические названия или фразы, чтобы сделать их проще для использования в речи или написании о технологиях. Акроним и аббревиатура являются сокращениями, составленными из первых букв последовательности слов, например: RADIUS (Remote Authentication Dial-In User Service) или TCP (Transmission Control Protocol). Если сокращение произносится как слово, как RADIUS ["РАДИУС"], то сокращение является акронимом. Если сокращение произносится по буквам, как TCP["Ти-Си-Пи"], то сокращение является аббревиатурой.

\*В этой книге все сокращения и акронимы по умолчанию пишутся на английском языке, например: TCP, MAC, за исключением очевидных сокращений на русском языке, например: ТД, БЛВС.

# История Беспроводных Локальных Вычислительных Сетей

В 19 веке, многочисленные изобретатели и ученые, включая Майкла Фарадея, Джеймса Клерка Максвелла, Генриха Рудольфа Герца, Николы Тесла, Дэвида Эдварда Хьюза, Томаса Эдисона, Гуэльельмо Маркони, и \*Александра Степановича Попова, начали экспериментировать с беспроводной связью. Эти изобретатели открыли и создали много теорий о концепции электромагнитных радиоволн [*radio frequency (RF)*].

Технология беспроводной сети была впервые использована военными США во время Второй Мировой Войны для передачи данных по радиосреде, используя секретную технологию шифрования, чтобы отправить боевые планы через вражеские линии. Технологии расширения радиоспектра, часто используемые в сегодняшних БЛВС, были также изначально запатентованы в эру Второй Мировой Войны, хотя они не применялись еще почти пару десятилетий спустя.

В 1970 году, Гавайский Университет [University of Hawaii] разработал первую беспроводную сеть, названную ALOHAnet [АЛОХАнет], чтобы обмениваться данными между Гавайскими Островами беспроводным способом. Сеть использовала протокол связи ЛВС 2ого уровня Взаимной Связи Открытых Систем [Open Systems Interconnection (OSI)], названным ALOHA [АЛОХА], в общей беспроводной среде в частотном диапазоне 400МГц. Технология, использованная в ALOHAnet часто считается "строительным блоком" для технологий Контроля Доступа к Среде [Medium Access Control (MAC)] Множественного Доступа с Контролем Несущей и Обнаружением Конфликтов [Carrier Sense Multiple Access with Collision Detection (CSMA/CD)], используемого в Ethernet, и Множественного Доступа с Контролем Несущей и Предотвращением Конфликтов [Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)], используемого в радиомодулях 802.11. Вы узнаете больше о CSMA/CA в Главе 8 "802.11 Доступ к Среде".

\*В этом параграфе и далее в книге аббревиатура MAC означает Medium Access Control, и произносится как [МАК].

В 1990-х коммерческие производители сетевого оборудования начали производить продукты для низкоскоростных беспроводных сетей передачи данных, большинство из которых работало в полосе частот 900 МГц. Институт Инженеров по Электротехнике и Электронике [Institute of Electrical and Electronics Engineers (IEEE)] начал обсуждать стандартизацию технологий БЛВС в 1991 году. В 1997 году IEEE принял первоначальный стандарт 802.11, который является фундаментом технологий БЛВС, о которых вы узнаете в этой книге.

Эта устаревшая технология 802.11 была развернута между 1997 и 1999 годами в основном на складах и производственных средах для использования низкоскоростного сбора данных с беспроводными сканерами штрих-кодов. В 1999 году IEEE определил более высокие скорости данных в поправке 802.11b. Введение скоростей передачи данных до 11Мбит/с вместе с уменьшением цены зажгли продажи беспроводных домашних сетевых маршрутизаторов на рынке небольших и домашних офисов [small office, home office (SOHO)]. Домашние пользователи вскоре привыкли к беспроводным сетям у себя дома, и начали запрашивать, чтобы их работодатели также предоставили возможности беспроводной сети на рабочих местах. После начального сопротивления технологии 802.11, небольшие компании, среднего размера бизнес и корпорации стали осознавать значение развертывания беспроводной сети 802.11 на своих предприятиях.

Если вы спросите среднестатистического пользователя о его беспроводной сети 802.11, он может на вас странно посмотреть. Название, которое люди чаще узнают для этой технологии – это *Wi-Fi*. *Wi-Fi* – это маркетинговый термин, узнаваемый во всем мире миллионами людей, обозначающий беспроводную сеть 802.11.

### Что означает термин *Wi-Fi*?

Много людей ошибочно считают, что *Wi-Fi* – это акроним от фразы *wireless fidelity* [*беспроводная точность воспроизведения*] (точно так же как *hi-fi* является сокращением от *high fidelity* [*высокая точность воспроизведения*]), но *Wi-Fi* это просто торговое название, используемое для рынка технологии БЛВС 802.11. Неопределенность в структуре стандартов IEEE для беспроводной связи позволяет производителям интерпретировать стандарт 802.11 различными способами. В результате, несколько производителей могут иметь IEEE 802.11-совместимые устройства, которые не совместимы друг с другом. Организация Альянс Совместимости Беспроводного Ethernet [Wireless Ethernet Compatibility Alliance (WECA)] была создана, чтобы точнее определить стандарт IEEE таким образом, чтобы привести к совместимости между производителями. WECA, теперь называется как *Wi-Fi* Альянс [*Wi-Fi Alliance*], выбрала термин *Wi-Fi* в качестве маркетингового бренда. Чемпионы *Wi-Fi* Альянса усиливают совместимость между беспроводными устройствами. Чтобы быть *Wi-Fi* совместимым, производитель должен отправить свои продукты в испытательную лабораторию *Wi-Fi* Альянса, которая тщательно протестирует на соответствие *Wi-Fi* сертификации. Больше информации о происхождении термина *Wi-Fi* можно найти на онлайн Сетевых Новостях *Wi-Fi* [*Wi-Fi Net News*]:

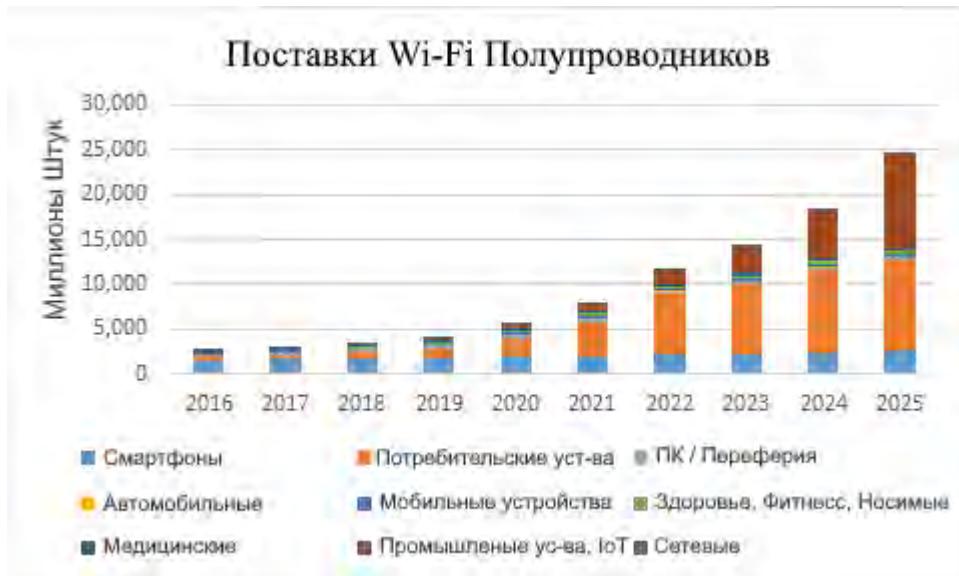
[https://wifinetnews.com/archives/2005/11/wi-fi\\_stands\\_for\\_nothing\\_and\\_everything.html](https://wifinetnews.com/archives/2005/11/wi-fi_stands_for_nothing_and_everything.html)

*Wi-Fi* радиомодули используются многочисленными приложениями предприятий и могут также быть найдены в ноутбуках, смартфонах, фотоаппаратах, телевизорах, принтерах, и многих других потребительских и промышленных устройствах. Согласно технологической исследовательской фирме Группа 650 [650 Group] ([www.650group.com](http://www.650group.com)), полупроводниковые поставки *Wi-Fi* радиомодулей превысили 4 миллиарда единиц в 2019 году. Как показано на Рисунке 1.1, поставки *Wi-Fi* радиомодулей продолжат расти дальше на миллиард в год. С того момента, когда первоначальный стандарт был создан в 1997 году, технология 802.11 выросла до огромных пропорций; *Wi-Fi* стал частью нашей общемировой культурой связи. Недавний отчет Телеком Эдвайзори Сервисез [Telecom Advisory Services] оценивает, что технологии, которые лежат на нелицензируемом спектре добавляют 222 миллиарда долларов США ежегодно к экономике США. Более 91 миллиарда долларов США можно отнести к *Wi-Fi*.

## Р И С У Н О К 1.1

## Рост Wi-Fi отрасли

Любезно предоставленный 650 Group



# Организации по Стандартам

Каждая организация по стандартам, обсуждаемая в этой главе, помогает вести разные аспекты беспроводной сетевой индустрии.

Сектор Радиосвязи Международного Союза Электросвязи и локальные организации, такие как Федеральная Комиссия по Связи в США [Federal Communications Commission (FCC)] или \*Государственная Комиссия по Радио Частотам (ГКРЧ) в России, устанавливают правила что пользователи могут делать с радиопередатчиками. Эти организации управляют и регулируют использование частот, уровней мощности и методы передачи. Они также работают вместе, чтобы помочь руководить ростом и расширением, которые запрашиваются пользователями беспроводной связи.

Институт Инженеров по Электротехнике и Электронике [Institute of Electrical and Electronics Engineers (IEEE)] создает стандарты для совместимости и сосуществования между сетевым оборудованием. Стандарты IEEE должны придерживаться правил организаций по связи, таких как FCC.

Подразделение Инженерных Задач Интернета [Internet Engineering Task Force (IETF)] ответственна за создание Интернет стандартов, или более академически - стандартов сетевого и межсетевого взаимодействия. Многие из этих стандартов интегрированы в беспроводные сети, и протоколы безопасности, и стандарты.

Wi-Fi Альянс проводит сертификационные испытания, чтобы гарантировать, что оборудование беспроводных сетей соответствуют руководящим документам по связи БЛВС 802.11, которые аналогичны стандарту IEEE 802.11-2020.

Международная Организация по Стандартизации [International Organization for Standardization (ISO)] создала модель Взаимосвязи Открытых Систем [Open Systems Interconnection (OSI)], которая является моделью архитектуры для обмена данными.

Следующие разделы обсуждают каждую из этих организаций более детально.

## Федеральная Комиссия по Связи

По-простому, Федеральная Комиссия по Связи [*Federal Communications Commission (FCC)*] регулирует связь внутри Соединенных Штатов, а также связь в и из Соединенных Штатов. Образованная Актом о Связи от 1934 года [*Communications Act of 1934*], FCC ответственна за регулирование связи между штатами и международную связь по радио, телевидению, телеграфу, спутнику, и кабелю. Задача FCC в беспроводных сетях – это регулировать радиосигналы, которые используются для беспроводных сетей. Юрисдикция FCC распространяется на 50 штатов, Округ Колумбия, и владения США. В большинстве стран есть государственные организации, который работают аналогично FCC.

FCC и соответствующие контролирующие агентства в других странах обычно регулируют две категории беспроводной связи: лицензируемый спектр и нелицензируемый спектр. Разница в том, что пользователи нелицензируемого спектра не должны проходить процедуру получения лицензии прежде, чем они смогут установить беспроводную систему. И лицензируемая и нелицензируемая связь обычно регулируется по следующим пятью областям:

- Частота
- Ширина полосы
- Максимальная мощность расчетного излучателя [*intentional radiator (IR)*]
- Максимальная эквивалентная изотропно излучаемая мощность (ЭИИМ) [*Maximum Equivalent Isotropically Radiated Power (EIRP)*]

equivalent isotropically radiated power (EIRP)]

- Использование (внутри помещений и/или снаружи)
- Правила совместного использования спектра

### Какие Преимущества и Недостатки Использования Нелицензируемых Частот?

Как ранее говорилось, лицензируемые частоты требуют утвержденную официальную лицензию, и финансовые затраты на это обычно очень высоки. Одно основное преимущество нелицензируемой частоты – это то, что разрешение на передачу на частоте бесплатно. Хотя финансовых затрат нет, вы все же должны придерживаться правил передачи и других ограничений. Другими словами, плата за передачу на нелицензируемой частоте может отсутствовать, но правила остаются.

Основной недостаток передачи в нелицензируемой полосе частот – это то, что кто-нибудь еще может также передавать в том же самом частотном пространстве. Нелицензируемые полосы частот часто очень переполнены; следовательно, передачи от других индивидуумов могут вызвать интерференцию с вашими передачами. Если кто-нибудь еще интерфеcирует с вашими передачами, то у вас нет юридических оснований для обращения за помощью до тех пор, пока другой индивидуум придерживается правил и постановлений для нелицензируемой частоты.

Фактически, FCC и другие регулирующие организации устанавливают правила что пользователь может делать относительно радиопередач. Отсюда, организации по стандартизации создают стандарты для работы согласно этим правилам. Эти организации работают вместе, чтобы помочь удовлетворить запросы от быстрорастущей беспроводной индустрии.

Правила FCC опубликованы в Своде Федеральных Нормативных Актов [Code of Federal Regulations (CFR)]. CFR поделен на 50 Книг, которые ежегодно обновляются. Книга, которая относится к беспроводным сетям – это Книга 47, *Телекоммуникации* [Title 47, *Telecommunication*]. Книга 47 поделена на много частей; Часть 15, “Радио Частотные Устройства” [Part 15, “Radio Frequency Devices”] – это где вы найдете правила и нормативные акты относительно беспроводных сетей, касающихся 802.11. Часть 15 далее разбита на подчасти и разделы. Полная ссылка будет выглядеть как следующий пример: 47CFR15.3. Электронный Свод Федеральных Нормативных Актов [Electronic Code of Federal Regulations (e-CFR)] это доступная в Интернете электронная версия CFR, которая доступна по следующему URL: [www.ecfr.gov](http://www.ecfr.gov).

## Международный Союз Электросвязи Сектор Радиосвязи

Существует глобальная иерархия для управления радиоспектром по всему миру. Организация Объединенных Наций поставила задачу *Международному Союзу Электросвязи Сектору Радиосвязи* [*International Telecommunication Union Radiocommunication Sector (ITU-R)*] по глобальному управлению спектром. ITU-R старается обеспечить без интерференционную связь на земле, море и в небе. ITU-R управляет базой данных назначения частот по всему миру по пяти административным регионам.

Пять административных регионов разбиты следующим образом:

**Регион А: Америка** Межамериканская Комиссия по Телекоммуникациям [Inter-American Telecommunication Commission (CITEL)]

[www.citel.oas.org](http://www.citel.oas.org)

**Регион В: Западная Европа** Европейская Конференция Управлений Почты и Телекоммуникаций [European Conference of Postal and Telecommunications Administrations (CEPT)]

[www.cept.org](http://www.cept.org)

**Регион С: Восточная Европа и Северная Азия** Региональное Содружество в Области Связи [Regional Commonwealth in the Field of Communications (RCC)]

[en.rcc.org.ru](http://en.rcc.org.ru)

**Регион D: Африка** Африканский Союз Телекоммуникаций [African Telecommunications Union (ATU)]

[www.atu-uat.org](http://www.atu-uat.org)

**Регион E: Азия и Австралия** Азиатско-Тихоокеанское Телесообщество [Asia-Pacific Telecommunity (APT)]

[www.apt.int](http://www.apt.int)

В дополнение к пяти административным регионам, ITU-R определяет три регуляторных радио региона. Эти три региона определяются географически, как показано на следующем списке. Вам стоит проверить официальную карту ITU-R, чтобы определить точные границы каждого региона.

- Регион 1: Европа, Средний Восток и Африка
- Регион 2: Америки
- Регион 3: Азия и Океания

Документы ITU-R, регулирующие радио, являются частью международного соглашения, регулирующего использование спектра. В каждом из этих регионов, ITU-R выделяет и назначает полосы частот и радио каналы, которые разрешены к использованию, а также условия касающиеся их использования. В каждом регионе, местные государственные организации регулирующие радиочастоты, такие как перечисленные ниже, управляют радиоспектром в своих странах:

**Австралия** Australian Communications and Media Authority (ACMA)

[www.acma.gov.au](http://www.acma.gov.au)

**Япония** Association of Radio Industries and Businesses (ARIB)

[www.arib.or.jp](http://www.arib.or.jp)

**Соединенные Штаты** Federal Communications Commission (FCC)

[www.fcc.gov](http://www.fcc.gov)

**\*Россия** Государственная Комиссия по РадиоЧастотам (ГКРЧ)

[digital.gov.ru/ru/activity/advisories/7](http://digital.gov.ru/ru/activity/advisories/7)

Важно понимать, что связь регулируется по-разному во многих регионах и странах. Например, Европейское радиорегулирование очень отличается от регулирования в Северной Америке. При развертывании БЛВС, пожалуйста, уделите время на изучение правил и политик местного регулирующего государственного органа [*regulatory domain authority*]. Однако, поскольку правила варьируются по всему миру, то перечисление ссылок на различные регулирующие правила выходят за пределы возможностей этой книги. Кроме того, экзамен CWNA не ссылается на радиорегулирование FCC или какой-либо другой определенной страны.

Больше информации о ITU-R можно найти на [www.itu.int/ITU-R](http://www.itu.int/ITU-R).

# Институт Инженеров Электротехники и Электроники

Институт Инженеров Электротехники и Электроники [*Institute of Electrical and Electronics Engineers*], обычно называемый *IEEE*, это глобальное профессиональное сообщество с более 420 000 членами в 160 странах. Миссия IEEE это “поощрение технологических инноваций и высокого качества на благо человечества.” Для сетевых профессионалов это означает создание стандартов, которыми мы пользуемся для связи.

IEEE, вероятно, лучше известен по своим стандартам ЛВС, проект IEEE 802.



Проект 802 это один из многих проектов IEEE; однако, в этой книге рассмотрен только один проект IEEE.

Проекты IEEE разделены на рабочие группы, чтобы разрабатывать стандарты, по определенным проблемам или потребностям. Например, рабочая группа IEEE 802.3 отвечала за создание стандарта Ethernet, а рабочая группа IEEE 802.11 отвечала за создание стандарта БЛВС. Номера назначаются по мере формирования групп, так номер 11, присвоенный рабочей группе, показывает, что это была 11ая рабочая группа, сформированная в проекте IEEE 802.

При возникновении необходимости пересмотреть существующие стандарты, созданные рабочими группами, формируются группы по решению определенных задач [task groups]. Этим группам по решению определенных задач [task group] присваивается последовательно одна буква (несколько букв присваивается, если все одиночные буквы уже использованы), которые добавляются в конце номера стандарта (например, 802.11a, 802.11g, и 802.3at). Некоторые буквы не назначаются. Например, о и l не назначаются, чтобы избежать путаницы с цифрами 0 и 1. Другие буквы могут не назначаться группам по решению определенных задач, чтобы избежать путаницы с другими стандартами. Например, 802.11x не назначается, потому что ее можно легко спутать со стандартом 802.1X, и потому что 802.11x стало общепринятой обычной ссылкой на семью стандартов 802.11.



Вы можете найти больше информации о IEEE на [www.ieee.org](http://www.ieee.org).

Важно помнить, что IEEE стандарты, как и многие другие стандарты, это написанные документы, описывающие как технические процессы и оборудование должно работать. К сожалению, это может привести к различной интерпретации, когда внедряется стандарт, поэтому для ранних продуктов возможна несовместимость между производителями, как в случае с некоторыми ранними продуктами 802.11



История стандарта 802.11 и поправок в значительной степени охвачена в Главе 2 “Стандарты и Поправки IEEE”. Экзамен CWNA (CWNA-108) основан на самой последней опубликованной версии стандарта, 802.11-2020. Стандарт 802.11-2020 можно загрузить здесь:

<https://standards.ieee.org>

## Подразделение Инженерных Задач Интернета

Подразделение Инженерных Задач Интернета [*Internet Engineering Task Force*], обычно называемое как *IETF*, это международное сообщество людей в сетевой отрасли, чья цель делать работу Интернет лучше. Миссия IETF, как определено организацией в документе с названием RFC 3935, это “создавать высококачественные, релевантные технические и инженерные документы, которые влияют на способ, которым люди проектируют, используют и управляют Интернетом, таким образом, чтобы сделать работу Интернета лучше. Эти документы включают стандарты протоколов, текущий передовой опыт, и информационные документы различных видов.” В IETF нет членских взносов, и любой может зарегистрироваться и посещать встречи IETF.

IETF – это одна из пяти главных групп, которые являются частью Интернет Сообщества [Internet Society (ISOC)]. Группы ISOC это:

- Подразделение Инженерных Задач Интернета [Internet Engineering Task Force (IETF)]
- Архитектурный Совет Интернета [Internet Architecture Board (IAB)]
- Интернет Корпорация по Назначению Имен и Номеров [Internet Corporation for Assigned Names and Numbers (ICANN)]
- Управляющая Инженерная Группа Интернета [Internet Engineering Steering Group (IESG)]
- Подразделение Исследовательских Задач Интернета [Internet Research Task Force (IRTF)]

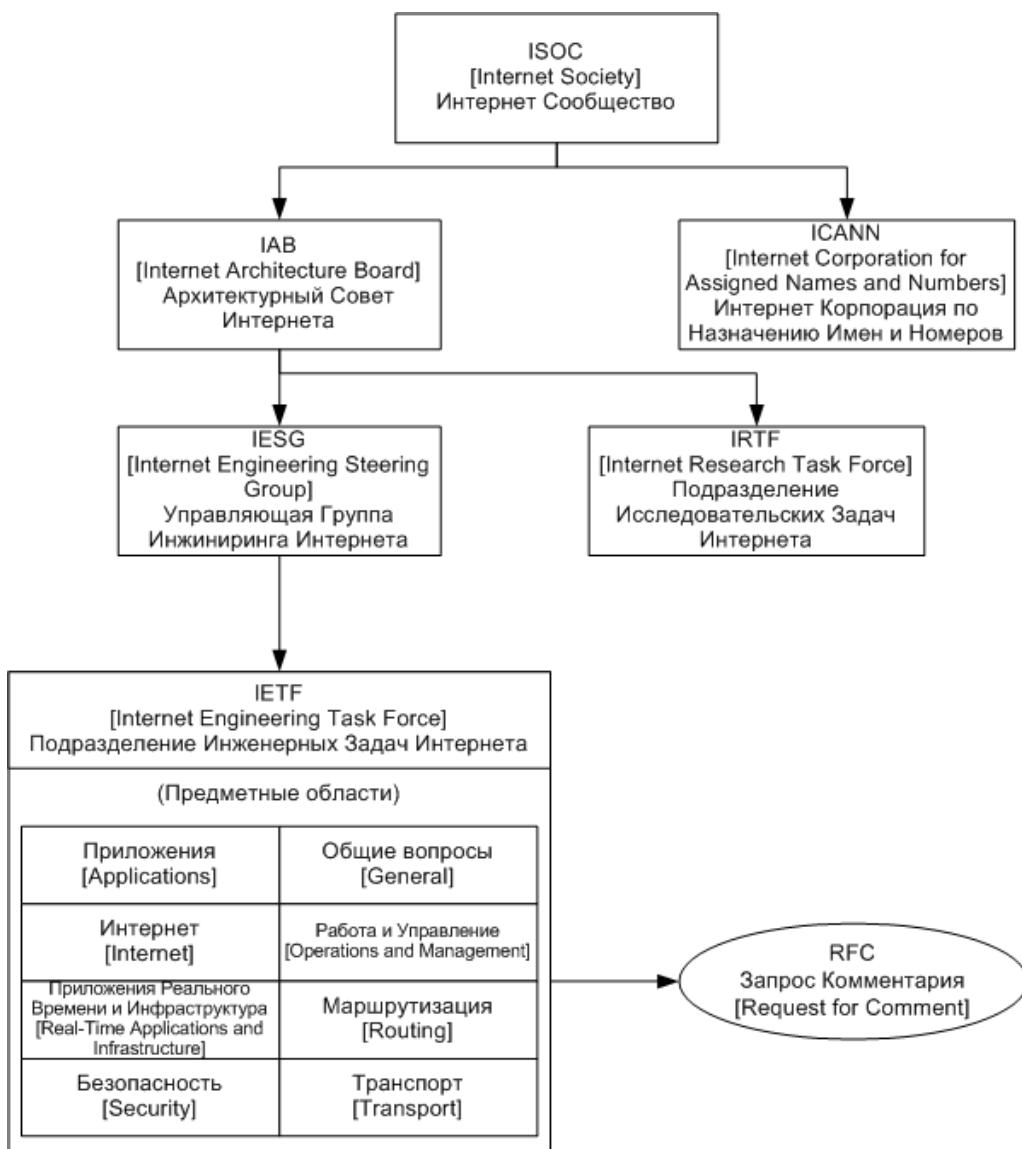
IETF разбит на восемь предметных областей: Приложения, Общие вопросы, Интернет, Работа и Управление, Приложения Реального Времени и Инфраструктура, Маршрутизация, и Транспорт. Рисунок 1.2 показывает иерархию ISOC и разбивку по предметным областям.

IESG обеспечивает техническое управление деятельностью IETF и продвижение Интернет стандартов. IETF сделан из большого числа групп, каждая из которых отвечает за определенные темы. Рабочая группа IETF создается IESG и ейдается определенное право или определенная тема для решения. В рабочих группах не существует формального процесса голосования. Решения в рабочих группах принимаются примерным консенсусом, или базовым общим смыслом соглашения внутри рабочей группы.

Результатами рабочей группы являются обычно документы с названием Запрос Комментариев [*Request for Comments (RFC)*]. В противоположность своему названию, RFC это в действительности не запрос комментариев, а утверждения и определения.

Большинство RFCs описывают сетевые протоколы, сервисы или политики, и могут развиться в Интернет стандарт. RFC нумеруются последовательно, и если номер назначен, то он никогда не используется повторно. RFCs могут быть обновлены или дополнены RFC с более высокими номерами. Например, Мобильный IPv4 был описан в RFC 3344 в 2002 году. Этот документ был обновлен в RFC 4636 и RFC 4721. В 2010 году, RFC 5944 сделал RFC

## РИСУНОК 1.2 Иерархия Интернет Сообщества (ISOC)



3344 вышедшим из употребления. В самом верху документа RFC указывается является ли RFC обновление другого RFC или делает другие RFC вышедшими из употребления.

Не все RFC являются стандартами. Каждому RFC дается статус, относительно его отношения с процессом Интернет стандартизации: Для информации [Informational], Экспериментальный [Experimental], Путь Стандартов [Standards Track], или Исторический [Historic]. Если это RFC на Пути Стандартов [Standards Track RFC], то он может быть Предложенным Стандартом [Proposed Standard], Черновым Стандартом

[Draft Standard], или Интернет Стандартом [Internet Standard]. Когда RFC становится стандартом, он сохраняет свой RFC номер, но ему также дается маркировка “STD xxxx”. Отношение между номерами STD и номерами RFC не один-в-один. STD номера идентифицируют протоколы, а RFC номера идентифицируют документы.

Многие из стандартов протоколов, текущего передового опыта, и информационных документов, созданных IETF, влияют на безопасность БЛВС. В Главе 17 “Архитектура Сетевой Безопасности 802.11” вы узнаете о некоторых вариациях Протокола Расширенной Аутентификации [Extensible Authentication Protocol (EAP)], который определен IETF RFC 3748, и как он определен для использования в БЛВС в IETF RFC 4017.

## Wi-Fi Альянс

*Wi-Fi Альянс* [*Wi-Fi Alliance*] – это глобальная некоммерческая отраслевая ассоциация с более чем 550 компаниями участниками, преданными продвижению роста БЛВС. Одна из первичных задач Wi-Fi Альянса это создание рынка бренда Wi-Fi и увеличению информированности потребителей о новых технологиях 802.11 по мере того, как они становятся доступными. Благодаря ошеломительному маркетинговому успеху Wi-Fi Альянса, большинство пользователей Wi-Fi по всему миру скорее всего узнают логотип Wi-Fi, который показан на Рисунке 1.3.

РИСУНОК 1.3

Логотип Wi-Fi



Главная задача Wi-Fi Альянса – это гарантировать совместную работу Wi-Fi продуктов путем проведения сертификационных испытаний. В ранние дни стандарта 802.11, Wi-Fi Альянс более детально определял некоторые неоднозначные требования стандартов и предоставлял набор руководств для обеспечения совместимости между различными производителями. Это продолжает выполняться, чтобы упростить сложность стандартов и обеспечить совместимость. Как показано на Рисунке 1.4, продукты, которые прошли процесс сертификации Wi-Fi получают Сертификат Совместимости Wi-Fi [Wi-Fi Interoperability Certificate], который предоставляет детальную информацию об индивидуальном продукте Wi-Fi Сертификации.

Wi-Fi Альянс, изначально называвшийся Альянс Совместимости Беспроводного Ethernet [Wireless Ethernet Compatibility Alliance (WECA)], был основан в Августе 1999 года. Название было изменено на Wi-Fi Альянс в Октябре 2002 года.

Wi-Fi Альянс сертифицировал более 50 000 Wi-Fi продуктов на совместимость с начала проведения испытаний в Апреле 2000 года. Существует несколько программ

СЕРТИФИЦИРОВАННЫЙ Wi-Fi [Wi-Fi CERTIFIED], охватывающих базовое соединение, безопасность, доступ и т.д. Тестирование продукции производителей Wi-Fi выполняется в независимых авторизованных испытательных лабораториях в семи странах. Список этих лабораторий можно найти на сайте Wi-Fi Альянса. Руководящие документы по совместимости по каждой программе СЕРТИФИЦИРОВАННЫЙ Wi-Fi [Wi-Fi CERTIFIED] обычно базируются на ключевых компонентах

## РИСУНОК1.4 Сертификат Совместимости Wi-Fi



## Wi-Fi CERTIFIED™ Interoperability Certificate

This certificate lists the features that have successfully completed Wi-Fi Alliance interoperability testing.  
Learn more: [www.wi-fi.org/certification/programs](http://www.wi-fi.org/certification/programs)



Certification ID: WFAXXXYYYY

Page 1 of 3

Date of Last Certification	January 01, 2013
Company	ABC Design
Product	Widget Series 123
Model Number	5678
Product Identifier(s)	AB-CDE-FG (SKU), 123456789 (UPC), AB123 (EAN), 131313TYTY (Other)
Category	Routers
Subcategory	Repeater, Extender, Mesh System, Controller
Hardware Version	Product: 11, Wi-Fi Component: 11
Firmware Version	Product: 11, Wi-Fi Component: 11
Operating System	Windows 8
Frequency Band(s)	2.4 GHz, 5 GHz, 60 GHz

## Summary of Certifications

CLASSIFICATION	PROGRAM
Connectivity	Wi-Fi CERTIFIED® a, b, g, n, ac Wi-Fi CERTIFIED 6™ Wi-Fi CERTIFIED WiGig™ WPA™ – Enterprise, Personal WPA2™ – Enterprise, Personal WPA3™ – Enterprise, Personal Wi-Fi Direct® Wi-Fi Enhanced Open™ TDLS
Optimization	Wi-Fi Agile Multiband™ Wi-Fi Data Elements™ Wi-Fi EasyMesh™ Wi-Fi Optimized Connectivity™ Wi-Fi TimeSync™ Wi-Fi Vantage™ WMM® WMM®-Admission Control WMM®-Power Save
Access	19SS with Wi-Fi Protected Setup™ Passpoint® Wi-Fi Easy Connect™ Wi-Fi Protected Setup™ Miracast™ - Display, Share
Applications & Services	Voice-Enterprise Voice-Personal Wi-Fi Aware™ Wi-Fi Location™ CWG-RF Test
RF Coexistence	



## Wi-Fi CERTIFIED™ Interoperability Certificate



**Certification ID: WFAXXXYYYY**

**Page 3 of 3**

**TDLS**

**Wi-Fi Agile Multiband™**

Steer to Cellular Data  
Fast Transition: WPA2-Enterprise <or> WPA2-Personal

**Wi-Fi Data Elements™**

**Wi-Fi EasyMesh™**

Release 1 or Release 2  
Channel Scan on request  
Wi-Fi EasyMesh Controller  
Wi-Fi EasyMesh Access Point  
Backhaul Link  
    Wi-Fi 2.4 GHz - Shared, Dedicated  
    Wi-Fi 5 GHz low band - Shared, Dedicated  
    Wi-Fi 5 GHz high band - Shared, Dedicated  
Ethernet  
Fronthaul Access Point  
    Wi-Fi 2.4 GHz - Shared, Dedicated  
    Wi-Fi 5 GHz low band - Shared, Dedicated  
    Wi-Fi 5 GHz high band - Shared, Dedicated  
Unassociated STA Link Metrics Reporting  
RCPI-based Steering

**Wi-Fi Optimized Connectivity™**

Fast Initial Link Setup Shared Key Authentication  
Higher Layer Protocol Encapsulation  
Estimated Service Parameters - (AP only)

**Wi-Fi TimeSync™**

**Wi-Fi Vantage™**

Release 1 or Release 2

**WMM™**

**WMM™-Admission Control**

**WMM™-Power Save**

**iBSS with Wi-Fi Protected Setup™**

**Passpoint™**

Release 1 or Release 2 or Release 3  
Online Signup (OSU) and Policy Provisioning  
Open Mobile Alliance™ Device Management (OMA DM)  
Wi-Fi Network Icon

**Wi-Fi Easy Connect™**

Bootstrapping-Human-Readable String  
Configurator  
Authentication Initiator Configurator  
Authentication Initiator Enrollee

**Wi-Fi Protected Setup™**

2.4 GHz, 5 GHz  
PIN  
Push-Button (PBC)  
NFC

**MiMcast™**

Release 1 or Release 2  
Display Device  
Source Device  
Content Protection

**Voice-Enterprise**

**Voice-Personal**

**Wi-Fi Aware™**

Enhanced Power-Saving  
Device Ranging  
Data Transfer (Native)  
Data Transfer (IP)  
Bluetooth® Low Energy Discovery Support

**Wi-Fi Location™**

<list applicable optional features based on application (STA or AP)>

**CWG-RF Test**

Please contact vendor for results.

**Spectrum and Regulatory Features**

802.11d  
802.11h

**Additional Capabilities**

BSS Max Idle Period  
Proxy ARP IPv4  
IPv6 Proxy Neighbor Discovery  
Directed Multicast Service



## Wi-Fi CERTIFIED™ Interoperability Certificate



Certification ID: WFAXXXYYYY

Page 2 of 3

## Security

WPA™ – Enterprise, Personal  
 WPA2™ – Enterprise, Personal  
 WPA3™ – Enterprise, Personal (Month Year Update)

## EAP Type(s)

- EAP-TLS
- EAP-TLS with RSA-3K-DHE
- EAP-TLS with RSA-3K-ECDHE
- EAP-TTLS/MSCAPv2
- PEAPv/EAP-MSCAPv2
- PEAP1/EAP-GTC
- EAP-SIM
- EAP-AKA
- EAP-AKA Prime
- EAP-FAST

## Any EAP Type

## 192-bit Security

Fast Transition for WPA3-Personal, WPA3-Personal transition mode, WPA3-Enterprise, WPA3-Enterprise transition mode

## Protected Management Frames

## Wi-Fi CERTIFIED™ a

## Wi-Fi CERTIFIED™ b

## Wi-Fi CERTIFIED™ e

## Wi-Fi CERTIFIED™ n

## 2.4 GHz, 5 GHz

X Spatial Streams 2.4 GHz

X Spatial Stream 5 GHz

Short Guard Interval 20 MHz

Short Guard Interval 40 MHz

Tx A-MPDU

STBC Receive

STBC Transmit

40 MHz operation in 2.4 GHz, with coexistence mechanisms

40 MHz operation in 5 GHz

HT Duplicate Mode (MCS 32)

OBSS on Extension Channel

Reduced Interframe Space (RIFS)

STAUT Power Management

## Wi-Fi CERTIFIED™ ac

X Spatial Stream 5 GHz

Rx MCS 8 (256-QAM)

Rx MCS 8-9 (256-QAM)

Tx STBC 2x1

Rx STBC 2x1

Rx A-MPDU of A-MSDU

Tx SU beamformer

Tx SU beamformer

Low Density Parity Check coding

Tx DL MU-MIMO

Rx DL MU-MIMO

Rx 160 MHz operation

Extended 5 GHz Channel Support

RTS with BW Signaling

## Wi-Fi CERTIFIED 6™

X Spatial Streams 2.4 GHz Rx  
 X Spatial Streams 5 GHz Rx  
 Maximum Supported Channel Width (20, 40, 80, 160 MHz)  
 DL MU-MIMO  
 8 Spatial Stream sounding  
 SU-MIMO with 2 SS  
 DL SU Beamforming  
 DL OFDMA  
 UL OFDMA  
 Target Wake Time (TWT)  
 MCS 8-9 Rx  
 MCS 10-11 Rx  
 MU-BAR trigger frame  
 MU-RTS / CTS trigger frame  
 DL MU-PPDU with basic trigger frame  
 Buffer Status Report (BSRP) trigger frame  
 256 Block Acknowledge (BA) Rx  
 256 Block Acknowledge (BA) Tx  
 MU EDCA Parameter set  
 Multiple-BSSID Set  
 Low Density Parity Check (LDPC) coding  
 Operating Mode Rx

## Wi-Fi CERTIFIED WiGig™

Extended MCS Support: 10 – 12

## Optional Features

2.4 GHz, 5 GHz  
 X Spatial Streams 2.4 GHz  
 X Spatial Stream 5 GHz  
 Short Guard Interval 20 MHz  
 Short Guard Interval 40 MHz  
 TX A-MPDU  
 STBC Receive  
 STBC Transmit  
 40 MHz operation in 2.4 GHz, with coexistence mechanisms  
 40 MHz operation in 5 GHz  
 HT Duplicate Mode (MCS 32)  
 OBSS on Extension Channel  
 Reduced Interframe Space (RIFS)  
 STAUT Power Management

## Wi-Fi Direct®

2.4 GHz, 5 GHz  
 Wi-Fi Direct Send – Transmit, Receive  
 Wi-Fi Direct for DLNA® – Transmit, Receive  
 Miracast – Display, Source  
 Wi-Fi Direct Print – Transmit, Receive  
 Wi-Fi Direct Toolkit

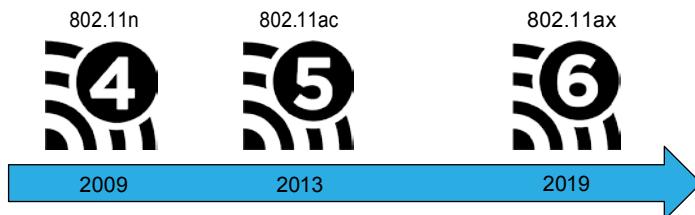
## Wi-Fi Enhanced Open™

ECC Group 20

и функционировании, которые определены в стандарте IEEE 802.11-2020 и в различных поправках 802.11. По факту, многие те же самые инженеры, кто принадлежит группам по решению конкретных задач 802.11 [802.11 task groups] также являются действующими членами Wi-Fi Альянса. Однако, важно понимать, что IEEE и Wi-Fi Альянс это две разные организации. Группы IEEE 802.11 по решению задач [IEEE 802.11 task group] определяют стандарты БЛВС, а Wi-Fi Альянс определяет сертификационные программы совместимости.

В прошлом, Wi-Fi Альянс называл свои базовые сертификации копируя соглашение о наименованиях, используемое IEEE. Например, сертификация *СЕРТИФИЦИРОВАННЫЙ Wi-Fi ac* [*Wi-Fi CERTIFIED ac*] проверяет радиомодули на соответствие рабочим характеристикам IEEE 802.11ac. Сертификация, *СЕРТИФИЦИРОВАННЫЙ Wi-Fi n* [*Wi-Fi CERTIFIED n*], проверяет радиомодули на соответствие рабочим характеристикам IEEE 802.11n. Недавно Wi-Fi Альянс принял новое соглашение по наименованиям по поколениям для Wi-Fi технологий. Цель в том, что новое соглашение по наименованиям будет легче для понимания для среднестатистического потребителя, в отличие от названий типа алфавитного винегрета, используемого IEEE. Поскольку технология 802.11ax как раз является таким основным сдвигом парадигмы от предыдущих версий технологии 802.11, то ей дали название поколения Wi-Fi 6. Старые версии технологии 802.11 также выстроили по этому новому соглашению о наименованиях. Например, 802.11ac можно называть Wi-Fi 5, а 802.11n - Wi-Fi 4, как показано на Рисунке 1.5.

**РИСУНОК 1.5** Поколения Wi-Fi



Многие другие сертификации Wi-Fi Альянса также проверяют на соответствие многие компоненты конкретной поправки 802.11; однако, наименование сертификации снова более дружелюбно потребителю, нежели чем название технического документа. Например, сертификация *Wi-Fi Мультимедиа* [*Wi-Fi Multimedia (WMM)*] опирается на механизмы QoS, которые изначально были определены в поправке IEEE 802.11e. В следующих разделах программы *СЕРТИФИЦИРОВАННЫЙ Wi-Fi* [*Wi-Fi CERTIFIED*] обсуждаются в контексте разных категорий. Все программы "СЕРТИФИЦИРОВАННОГО Wi-Fi" ["*Wi-Fi CERTIFIED*"] обратно совместимы с ранними версиями Wi-Fi, работающими на той же самой полосе частот.

## Подключение

### **СЕРТИФИЦИРОВАННЫЙ Wi-Fi 6 [Wi-Fi CERTIFIED 6]**

Wi-Fi Альянс сертифицирует рабочие характеристики радиомодулей 802.11ax для обеих полос частот 2.4 ГГц и 5 ГГц. *СЕРТИФИЦИРОВАННЫЕ Wi-Fi 6* устройства обеспечивают большую емкость, многогигабитные скорости передачи данных, лучшую энергоэффективность, и

высокую производительность, даже в плотно заполненных средах. Эти радиомодули обратно совместимы с радиомодулями 802.11ac и 802.11n. Глубокое обсуждение 802.11ax можно найти в Главе 19 “802.11ax: Высокая Эффективность.” Wi-Fi Альянс также анонсировал Wi-Fi 6E как “расширение” для сертификации характеристик и возможностей 802.11ax Wi-Fi 6 в 6ГГц полосе. Федеральная Комиссия по Связи Соединенных Штатов недавно утвердила 1200 МГц в 6ГГц полосе для нелицензируемого использования, а технология Wi-Fi 6 будет доступна в этой полосе с 2021 года. Больше информации о Wi-Fi в 6 ГГц полосе частот можно найти в Главе 6 "Беспроводные Сети и Технологии Расширения Спектра".

**СЕРТИФИЦИРОВАННЫЙ Wi-Fi ac [Wi-Fi CERTIFIED ac]** Wi-Fi Альянс сертифицирует рабочие характеристики радиомодулей 802.11ac для полосы частот 5 ГГц. Технология 802.11ac представила следующие улучшения уровней PHY и MAC, чтобы достичь более высоких скоростей передачи данных по сравнению с 802.11n. Радиомодули 802.11ac обратно совместимы с радиомодулями 802.11a/n. Глубокое обсуждение 802.11ac можно найти в Главе 10 “Технология MIMO: HT и VHT.”

**СЕРТИФИЦИРОВАННЫЙ Wi-Fi n [Wi-Fi CERTIFIED n]** Wi-Fi Альянс сертифицирует рабочие характеристики для радиомодулей 802.11n для обеих полос частот 2.4 ГГц и 5 ГГц. 802.11n представил улучшения уровней PHY и MAC для получения более высоких скоростей передачи данных. 802.11n требует радио системы *много-входов, много-выходов* [*multiple-input, multiple-output (MIMO)*], которые обратно совместимы с технологией 802.11a/b/g. Глубокое обсуждение 802.11n можно найти в Главе 10.

#### **СЕРТИФИЦИРОВАННЫЙ Wi-Fi WiGig [Wi-Fi CERTIFIED WiGig]**

Сертификационная программа WiGig основана на технологии, изначально определенной в поправке 802.11ad для *направленных мульти-гигабитных* [*directional multi-gigabit (DMG)*] радиомодулей, которые передают в полосе частот 60 ГГц. Многополосные СЕРТИФИЦИРОВАННЫЕ W-Fi WiGig устройства могут незаметно переключать передачу между полосами 2.4, 5, и 60 ГГц. Рабочие параметры определены в технической спецификации 60 ГГц Wi-Fi Альянса. WiGig использует широкие каналы в 60 ГГц, чтобы передавать данных фактически со скоростью в несколько гигабит в секунду и с низкой задержкой на расстоянии до 10 метров. Примеры использования WiGig включают беспроводные стыковочные или док станции, потоковое HD видео, и другие приложения с интенсивным использованием полосы.

**Прямое подключение Wi-Fi [Wi-Fi Direct]** *Прямое подключение Wi-Fi [Wi-Fi Direct]* позволяет Wi-Fi устройствам подключаться напрямую без использования точки доступа (ТД), делая проще возможность печати на принтере, обмена файлами, синхронизироваться, и выводить изображение на экран. Прямое подключение Wi-Fi [Wi-Fi Direct] идеально для мобильных телефонов, фото и видео камер, принтеров, ПК, и игровых устройств, которым необходимо устанавливать соединение один-к-одному, или даже соединять небольшую группу устройств. Прямое подключение Wi-Fi [Wi-Fi Direct] просто настраивать (в некоторых случаях это просто нажать кнопку), предоставляет ту же самую производительность и дальность, что и другие СЕРТИФИЦИРОВАННЫЕ Wi-Fi [Wi-Fi CERTIFIED] устройства, и защищено с помощью безопасности WPA2. Прямое подключение Wi-Fi [Wi-Fi Direct] применяет технологию, основанную на технической спецификации Wi-Fi Равный-с-Равным [Wi-Fi Peer-to-Peer].

## **Безопасность**

### **СЕРТИФИЦИРОВАННЫЙ Wi-Fi WPA3 [Wi-Fi CERTIFIED WPA3]**

Защищенный Wi-Fi Доступ 3 [Wi-Fi Protected Access 3 (WPA3)] определяет улучшения к существующим характеристикам безопасности WPA2 для радиомодулей 802.11. Он поддерживает новые методы безопасности, не разрешает старые устаревшие методы, и требует использования Защищенных Кадров Управления [Protected Management Frames (PMF)] для поддержки устойчивости жизненно-важных сетей. Персональный WPA3 [WPA3-Personal] с выгодой для себя использует Одновременную Аутентификацию Равных [Simultaneous Authentication of Equals (SAE)] для предоставления более сильной защиты для пользователей от атак подбора паролей. Корпоративный WPA3 [WPA3-Enterprise] предлагает эквивалент 192-битной криптографической силы. Вы найдете более детальное обсуждение безопасности WPA3 в Главе 17.

### **СЕРТИФИЦИРОВАННЫЙ Wi-Fi WPA2 [Wi-Fi CERTIFIED WPA2]**

Сертификация Защищенный Wi-Fi Доступ 2 [Wi-Fi Protected Access 2 (WPA2)] основана на возможностях *надежно защищенной сети* [*robust security network (RSN)*], механизмах безопасности, которые были определены в поправке IEEE 802.11i. Все сертифицированные Wi-Fi WPA2 устройства должны поддерживать динамические методы шифрования CCMP/AES. Wi-Fi Альянс определяет два метода для авторизации пользователей и устройств в БЛВС. *Корпоративный WPA2 [WPA2 Enterprise]* требует поддержку безопасности контроля доступа на основе портов 802.1X при установках на предприятиях. *Персональный WPA2 [WPA2-Personal]* использует менее сложный метод с паролем, предназначенный для сред малых и домашних офисов [SOHO]. Вы найдете более детальное обсуждение безопасности WPA2 и WPA3 в Главе 17.

**Улучшенный Открытый Wi-Fi [Wi-Fi Enhanced Open]** Эта сертификация основана на Гибком Беспроводном Шифровании [*Opportunistic Wireless Encryption (OWE)*] и обеспечивает защиту пользователей от пассивного подслушивания, когда нет требования к пользователям вводить пароль или парольную фразу для присоединения к сети. Он совмещает установленные криптографические механизмы для предоставления каждому пользователю уникального индивидуального шифрования, защищающего обмен данными между пользователем и точкой доступа. Больше информации о OWE можно найти в Главе 17.

**Защищенные Кадры Управления [Protected Management Frames]** Эта сертификация основана на поправке IEEE 802.11w-2009. Это поправка о *защите кадров управления* [*management frame protection (MFP)*], с целью доставки определенных типов кадров управления безопасным способом. Предназначение в том, чтобы предотвратить подделку [spoofing] определенных типов кадров управления 802.11 и предотвратить типовые атаки отказа в обслуживании на 2ом уровне [*layer 2 denial-of-service (DoS) attacks*].

## Доступ

**Пасспоинт [Passpoint]** *Пасспоинт [Passpoint]* спроектирован, чтобы революционизировать опыт конечного пользователя при подключении к Wi-Fi хотспотам. Он автоматически идентифицирует провайдера хотспота и подключается к нему, автоматически аутентифицируя пользователя в сети с помощью Протокола Расширенной Аутентификации [Extensible Authentication Protocol (EAP)], и обеспечении безопасной передачи с помощью безопасности WPA2-Enterprise или WPA3-Enterprise. Passpoint основан на технической спецификации *Хотспот 2.0 [Hotspot 2.0]*. Более подробную информацию о Пасспоинте [Passpoint] и Хотспоте [Hotspot] можно найти в Главе 18 “Приноси Свое Собственное Устройство (BYOD) и Гостевой Доступ.”

**Wi-Fi Простой Контакт [Wi-Fi Easy Connect]** *Wi-Fi Простой Контакт [Wi-Fi Easy Connect]* предоставляет возможность быстро и легко настроить устройства и обеспечить необходимым, путем сканирования QR кода продукта или читаемой строки. Сканирующее устройство должно запустить *Протокол Обеспечения Устройства [Device Provisioning Protocol (DPP)]*, разработанный Wi-Fi Альянсом. Оно использует публичные ключи шифрования для обеспечения безопасной аутентификации, и поддерживает обеспечение сетей WPA2 и WPA3.

**Защищенная Установка Wi-Fi [Wi-Fi Protected Setup]** *Защищенная Установка Wi-Fi [Wi-Fi Protected Setup (WPS)]* определяет упрощенную и автоматическую настройку безопасности WPA и WPA2 для домашних пользователей и пользователей малого бизнеса. Пользователи могут просто настроить сеть с защитой безопасности с помощью близкополевой связи [near field communication (NFC)], персональным идентификационным номером [personal identification number (PIN)], или кнопки, расположенной на ТД и клиентском устройстве. Технология WPS определена в технической спецификации Простая Конфигурация Wi-Fi [Wi-Fi Simple Configuration].

## Приложения и Сервисы

**Миракаст [Miracast]** *Miracast* незаметно подключает экраны потокового контента высокого разрешения [high-definition (HD)] и Ультра Высокого-Разрешения [Ultra High-Definition (Ultra HD)] между устройствами. Беспроводные каналы связи используются для замены проводных соединений. Устройства спроектированы для идентификации и подключения друг к другу, управления своими соединениями, и оптимизацией передачи видеоконтента. Miracast основан на Технической Спецификации Wi-Fi Экран [Wi-Fi Display Technical Specification].

Сертификационная программа Miracast предназначена для любых видео устройств, таких как камеры, телевизоры, проекторы, планшеты и смартфоны. Спаренные по Miracast устройства могут передавать поток HD или Ultra HD контента или зеркалировать экраны по Wi-Fi соединению равный-с-равным.

**Голосовая связь для Предприятий [Voice-Enterprise]** *Voice-Enterprise* предлагает улучшенную поддержку для голосовых приложений в корпоративных Wi-Fi сетях. Оборудование голосовой связи уровня предприятий должна обеспечивать постоянно хорошее качество голоса при всех условиях сетевой загрузки и сосуществовать с трафиком данных. Многие механизмы, определенные поправками IEEE 802.11k,

22        Глава 1 • Обзор Беспроводных Стандартов, Организаций, и Основ  
802.11r, и 802.11v также определены сертификацией Голосовая связь для  
Предприятий [Voice-Enterprise]. И точка доступа, и клиентские устройства должны  
поддерживать приоритезацию с помощью Wi-Fi Мультимедиа [Wi-Fi Multimedia  
(WMM)], с размещением голосового трафика в очередь с наивысшим приоритетом  
(Категория Доступа Голос, AC\_VO) [(Access Category Voice, AC\_VO)]. Оборудование  
корпоративной голосовой связи [Voice-Enterprise equipment] должно также  
поддерживать незаметное переключение (бесшовный роуминг) между ТД,  
безопасность WPA2-Enterprise, оптимизацию мощности через механизм Экономии  
Энергии WMM [WMM-Power Save], и управление трафиком через Контроль  
Допуска к Ресурсам WMM [WMM-Admission Control].

**Осведомленность о Wi-Fi [Wi-Fi Aware]**      Осведомленность о Wi-Fi [Wi-Fi Aware]  
позволяет устройствам использовать энерго-эффективное обнаружение рядом  
находящихся сервисов или информации перед созданием соединения. Техническая  
спецификация *сеть информированности о соседях [neighbor awareness networking  
(NAN)]* определяет механизмы для устройств БЛВС, чтобы синхронизировать  
информацию о канале и времени, для принятия во внимание сервисами  
обнаружения. *Wi-Fi Осведомленность [Wi-Fi Aware]* не требует наличия  
инфраструктуры БЛВС, и обнаружение происходит в фоновом режиме, даже в  
переполненных пользователями средах. До установления соединения, пользователи  
могут найти других рядом находящихся пользователей в целях обмена фото и видео  
материалами, местной информации и оппонентов по игре.

**Wi-Fi Местоположение [Wi-Fi Location]**      *Wi-Fi Местоположение [Wi-Fi  
Location]* основано на протоколе Измерения Точного Времени [Fine Timing  
Measurement (FTM)], изначально определенного в стандарте IEEE 802.11-2016.  
Устройства и сеть с включенным местоположением по Wi-Fi [Wi-Fi Location]  
может предоставить устройствам информацию о местоположении внутри помещений с  
высокой точностью через Wi-Fi сеть без необходимости установленной поверх  
инфраструктуры, такой как iBeacons или системы определения местоположения в  
реальном времени [real-time locating system (RTLS)]. Разработчики Приложений и ОС  
могут создать приложения и сервисы на основе местоположений. Некоторые  
потенциальные применения включают управление инвентарем, геозонирование  
[geofencing], и гиперлокальный маркетинг.

## Оптимизация

### **Установка Туннелированного Прямого Канала Связи [Tunneled Direct Link Setup]**

Поправка IEEE 802.11z-2010 определяет протокол безопасности Установка Туннелированного Прямого Канала Связи [*Tunneled Direct Link Setup (TDLS)*]. Wi-Fi Альянс также представил TDLS как программу сертификации для устройств, использующих TDLS для прямого подключения друг к другу, после того как они присоединились к традиционной Wi-Fi сети. Это позволяет таким потребительским устройствам, как телевизоры, игровые приставки, смартфоны, камеры и принтеры, прямо и безопасно связываться друг с другом, оставаясь при этом подключенными к точке доступа.

**Умная Многополосность Wi-Fi [Wi-Fi Agile Multiband]** **Умная Многополосность Wi-Fi [Wi-Fi Agile Multiband]** обеспечивает лучшее управление средами Wi-Fi сетей, позволяя Wi-Fi устройствам реагировать на изменения условий Wi-Fi сети. Клиентские устройства могут обмениваться информацией с инфраструктурными устройствами, позволяя точкам доступа принимать разумные решения о выборе полосы и канала, избегать перегруженных полос, минимизировать прерывание сервиса, и предоставлять Wi-Fi сервис высокого качества независимо от изменений в среде.

**Элементы Данных Wi-Fi [Wi-Fi Data Elements]** **Элементы Данных Wi-Fi [Wi-Fi Data Elements]** образуют стандартизированную модель для доставки 130 определенных ключевых показателей производительности сети Wi-Fi. Этот последовательный подход поможет с решением проблем и поможет лучше понять проблемы заказчиков. Элементы Данных Wi-Fi [Wi-Fi Data Elements] также предоставляют необходимую основу для сетей Wi-Fi Простой Взаимосвязности [Wi-Fi EasyMesh].

**Простая Взаимосвязь Wi-Fi [Wi-Fi EasyMesh]** **Простая Взаимосвязь Wi-Fi [Wi-Fi EasyMesh]** предоставляет простой в использовании, самоадаптирующийся и гибкий подход к нескольким точкам доступа, которые работают вместе в домашних и небольших офисных Wi-Fi сетях. Простая Взаимосвязь Wi-Fi [Wi-Fi EasyMesh] делает простым установку сети и подключение устройств, требуя минимального пользовательского вмешательства.

### **Оптимизированное Подключение к Wi-Fi [Wi-Fi Optimized Connectivity]**

*Оптимизированное подключение к Wi-Fi [Wi-Fi Optimized Connectivity]* предоставляет пользователям мобильных устройств еще более незаметное подключение путем оптимизации процесса обнаружения Wi-Fi сетей, установки подключения, и гарантирует пользователям, что они подключены к лучшей ТД, по мере того как они переключаются между точками доступа. Ключевые выгоды включают оптимизированное обнаружение сетей, стандартизированная оценка качества канала связи, оптимизированная аутентификация и плавные передачи.

**Преимущество с Wi-Fi [Wi-Fi Vantage]** **Растущая тенденция в Wi-Fi отрасли - когда провайдеры управляемых услуг [managed service provider (MSP)] предлагают "беспроводную сеть как услугу" ["wireless as a service."]** Многие операторы связи предлагают MSP услуги, которые следят за работой Wi-Fi в аэропортах, на стадионах, в школах, офисных зданиях, на территории торговых сетей и гостиниц, и на других местах сбора людей. **Преимущество с Wi-Fi [Wi-Fi Vantage]** нацелено на улучшение впечатлений от использования для пользователей в управляемых Wi-Fi сетях.

**WMM (Wi-Fi Мультимедиа) [WMM (Wi-Fi Multimedia)]** *Wi-Fi Мультимедиа [Wi-Fi Multimedia (WMM)]* основано на механизмах QoS, которые изначально были определены в поправке IEEE 802.11e. WMM позволяет Wi-Fi сетям приоритезировать трафик, генерируемый разными приложениями. В сети, где WMM поддерживается и ТД и клиентским устройством, трафик, создаваемый такими чувствительными ко времени приложениями, как голос или видео, могут быть приоритезированы для передачи по полудуплексной радиосреде. Сертификация WMM обязательна для всех сертифицированных устройств ядра, которые поддерживают 802.11n и 802.11ac. Сертификация WMM является optionalной для сертифицированных устройств ядра, которые поддерживают 802.11 a, b, или g. Механизмы WMM обсуждаются более детально в Главе 9 “802.11 MAC.”

**Контроль Допуска к WMM [WMM-Admission Control]** *Контроль Допуска к WMM [WMM-Admission Control (WMM-AC)]* позволяет Wi-Fi сетям управлять трафиком на основе состояния канала, загрузки сетевого трафика, и типа трафика (голос, видео, негарантированные данные, или фоновые данные). Точка доступа разрешает подключить к сети только трафик, который она может поддерживать, на основе доступных сетевых ресурсов. WMM-AC использует механизмы *контроля допуска вызовов [call admission control (CAC)]* для предотвращения переподписки голосовых вызовов через точку доступа 802.11.

**ЭнергоСбережение WMM [WMM-Power Save]** *Энергосбережение WMM [WMM-Power Save (WMM-PS)]* помогает сберечь заряд аккумуляторной батареи для устройств, использующих Wi-Fi радиомодули, путем управления временем, которое клиентское устройство проводит в спящем режиме. Сохранение жизни аккумулятора является критичным для ручных устройств таких, как сканер штрихкодов и телефоны с передачей голоса через Wi-Fi [voice over Wi-Fi (VoWiFi)]. Чтобы использовать преимущества возможностей энергосбережения и устройство, и точка доступа должны поддерживать WMM-PS. Глава 9 обсуждает WMM-PS и устаревшие механизмы сбережения энергии более подробно.

## Радиочастотное Существование

**CWG-RF** *Группа Совмещенной Беспроводной связи - РЧ Профиль [Converged Wireless Group-RF Profile (CWG-RF)]* была образована совместно Wi-Fi Альянсом и Ассоциацией Сотовой Связи и Интернета [Cellular Telecommunications and Internet Association (CTIA)]. CWG-RF определяет метрики производительности и тестирования для Wi-Fi и сотовых радиомодулей в совмешенных трубках, чтобы помочь гарантировать, что обе технологии работают хорошо в присутствии друг друга. Хотя программа испытаний не является элементом сертификации Wi-Fi, выполнение испытаний является обязательным для телефонов с Wi-Fi.

## Дополнительные Возможности

**Энергосберегающие Характеристики [Power-Saving Features]** *Энергосберегающие характеристики [Power-saving features]* - это новые набор возможностей по увеличению срока жизни аккумулятора в Wi-Fi устройствах. Энергетическая эффективность получается за счет увеличения периодов сна и уменьшения периодов связи между клиентами и сетью.

**Проект Домашнего Wi-Fi [Wi-Fi Home Design]** *Проект Домашнего Wi-Fi [Wi-Fi Home Design]* позволяет строителям новых домов предлагать профессионально спроектированный, сделанный "под ключ", высокопроизводительный Wi-Fi, встроенный прямо в новые построенные дома и многоквартирные дома такие, как кондоминимумы, таунхаусы и комплексы апартаментов.

## Будущие Сертификации

По мере развития технологий 802.11, новые программы СЕРТИФИЦИРОВАННОГО Wi-Fi [Wi-Fi CERTIFIED] будут определяться Wi-Fi Альянсом. Например, *Wi-Fi HaLow* это предлагаемая сертификация, предназначенная для маломощных устройств, работающих на частотах ниже 1 ГГц и с большей дальностью работы. Wi-Fi HaLow основан на поправке IEEE 802.11ah, предназначеннной для устройств Интернета Вещей [*Internet of Things (IoT)*]. Wi-Fi Альянс исследует соответствие автоматизированной координации частот [*automated frequency coordination (AFC)*] согласно законодательству и определенные требования Wi-Fi для 6 ГГц спектра. Больше информации о AFC и 6 ГГц полосе частот можно найти в Главе 6.

Планы развития, так называемая дорожная карта, Wi-Fi Альянса включает обновление версий существующих сертификаций, а также сертификаций, которые могут быть нацелены на работу Wi-Fi, характерные для вертикальных отраслей.

Также как стандартам и поправкам IEEE 802.11, технологиям, определенным в новых сертификационных программах Wi-Fi Альянса, нужно много лет, прежде чем они станут широко распространенными на рынке.

### Wi-Fi Альянс и Программы Wi-Fi Сертификации

Узнайте больше о Wi-Fi Альянсе на [www.wi-fi.org](http://www.wi-fi.org). Вебсайт Wi-Fi Альянса содержит много статей, ответов на часто задаваемые вопросы [FAQs], и информационные листовки [white papers], описывающие организацию вместе с дополнительной информацией по сертификационным программам. Технические информационные листовки [white papers] Wi-Fi Альянса рекомендуются для дополнительного чтения при подготовке к экзамену CWNA. Wi-Fi Альянс также поддерживает базу данных сертифицированных Wi-Fi продуктов с возможностью поиска. Пройдите на [www.wi-fi.org/product-finder](http://www.wi-fi.org/product-finder), чтобы проверить статус сертификации любого Wi-Fi устройства.

## Международная Организация по Стандартизации

Международная Организация по Стандартизации [*International Organization for Standardization*], обычно называемая ISO, это всемирная негосударственная организация, которая определяет потребности бизнеса, государства, и общества и разрабатывает стандарты в партнерстве с секторами, в которых это будет применяться. ISO отвечает за создание модели Взаимосвязи Открытых Систем [*Open Systems Interconnection (OSI)*], которая была стандартной моделью для связи по передаче данных между компьютерами с конца 1970х.

### Почему ISO, а не IOS?

/ISO это не ошибочно набранные инициалы. Это слово, полученное от Греческого слова *isos*, которое означает *равный или одинаковый*. Поскольку инициалы могут отличаться от страны к стране, из-за различий в переводах, ISO решила использовать слово вместо инициалов в своем названии. Зная это, легко понять, почему организация по стандартизации дала себе имя, которое означает одинаковый.

Модель OSI является краеугольным камнем в области передачи данных, и изучение, для ее понимания, является одной из самых важных и фундаментальных задач, которую человек в сетевой отрасли может попытаться решить. Рисунок 1.6 показывает семь уровней модели OSI.

Стандарт IEEE 802.11-2020 определяет механизмы связи только на Физическом уровне и MAC подуровне Канального [Data-Link] уровня модели OSI. Как используется технология 802.11 на этих двух уровнях OSI обсуждается детально в этой книге.

**Р И С У Н О К 1 . 6**      Семь уровней модели OSI



У вас должны быть рабочие знания модели OSI и для этой книги, и для экзамена CWNA. Удостоверьтесь, что вы понимаете семь уровней модели OSI и как осуществляется связь на разных уровнях. Если вы не уверены в своих знаниях концепции модели OSI, потратьте немного времени на знакомство с ней в Интернете или из хороших книг по основам сетей прежде, чем проходить экзамен CWNA. Больше информации о ISO можно найти на [www.iso.org](http://www.iso.org).

# Ядро, Распределение и Доступ

Если вы когда-либо проходили курс по сетям или читали книгу о проектировании сетей, вы вероятно слышали термины **ядро [core]**, **распределение [distribution]** и **доступ [access]**, при обращении к сетевой архитектуре. Надлежащий сетевой дизайн или проект обязателен, не зависимо от типа используемой сетевой топологии. Ядро сети - это высокоскоростная опорная сеть или высокоскоростная магистраль сети. Цель ядра - переносить большое количество информации между ключевыми центрами обработки данных или областями распределения, также как высокоскоростные магистрали соединяют большие города и городские округа.

Уровень ядра не маршрутизирует трафик и не манипулирует пакетами, а выполняет высокоскоростную коммутацию. Решения по резервированию и избыточности обычно проектируются на уровне ядра, чтобы гарантировать быструю и надежную доставку пакетов. Уровень распределения сети маршрутизирует или направляет трафик на небольшие кластеры узлов или соседств сети.

Уровень распределения маршрутизирует трафик между виртуальными ЛВС [virtual LANs (VLANs)] и подсетями. Уровень распределения похож на штат(регион) и региональные дороги, которые обеспечивают среднюю скорость движения и распределяют трафик внутри больших городов и городских округов.

Уровень доступа сети отвечает за медленную доставку трафика прямо конечному пользователю или конечному узлу. Уровень доступа похож на дороги местного значения и соседние улицы, которые используются чтобы добраться до вашего итогового адреса. Уровень доступа обеспечивает финальную доставку пакетов конечному пользователю. Помните, что скорость является относительной.

Из-за загрузки трафика и запросов на пропускную способность, возможности по скорости и пропускной способности возрастают по мере движения данных с уровня доступа на уровень ядра. Тенденция к увеличению скорости и пропускной способности также означает более высокую стоимость.

Так же как не практично строить высокоскоростную магистраль для трафика между вашим двором и местной школой, не будет практическим или эффективным строительство двухполосной дороги в качестве главной дороги, соединяющей два больших города, таких как Нью-Йорк и Бостон. Эти же самые принципы применимы и к сетевому дизайну. Каждый сетевой уровень—ядро [core], распределение [distribution], и доступ [access]—спроектирован для обеспечения определенных функций и возможностей для сети. Важно понимать как беспроводная сеть подходит к этой модели сетевого дизайна..

Беспроводная сеть может быть установлена как решение точка-точка или точка-многоточка. Большинство беспроводных сетей используются для предоставления сетевого доступа индивидуальным клиентским станциям, и проектируются как сети точка-многоточка. Этот тип применения проектируется и устанавливается на уровне доступа, предоставляющего подключение конечному пользователю. Беспроводные сети 802.11 наиболее часто устанавливаются на уровне доступа, в которых клиенты БЛВС поддерживают связь через стратегически установленные точки доступа.

Каналы связи через беспроводные мосты обычно используются для предоставления связи между зданиями, тем же самым способом, как региональные и государственные дороги предоставляют распределение трафика между соседями. Назначение беспроводных мостов в соединении двух отдельных проводных сетей беспроводным способом. Маршрутизация трафика данных между сетями обычно ассоциируется с

28 Глава 1 • Обзор Беспроводных Стандартов, Организаций, и Основ уровнем распределения. Каналы связи через беспроводные мосты обычно не удовлетворяют требованиям по скорости и расстоянию для уровня ядра, но они могут быть очень эффективны на уровне распределения. Канал связи через мост 802.11 является примером беспроводной технологии, развернутой на уровне распределения.

Хотя беспроводная связь обычно не ассоциируется с уровнем ядра, вы должны помнить, что требования по скорости и расстоянию очень сильно отличаются между большими и малыми компаниями, и что уровень распределения одной может быть уровнем ядра другой. Совсем небольшие компании могут даже применять беспроводную сеть для всех сетевых устройств конечных пользователей, отказываясь от любых проводных устройств, кроме соединения в Интернет. Проприетарные беспроводные мосты с более высокой шириной полосы и некоторые установки взаимосвязываемых [mesh] сетей 802.11 можно считать применением беспроводной связи на уровне ядра.

### Логические Плоскости Телекоммуникаций

Телекоммуникационные сети часто определяются тремя логическими плоскостями работы: управления, контроля и данных. *Плоскость управления [management plane]* существует для мониторинга и администрирования телекоммуникационной сети. *Плоскость контроля [control plane]* характеризуется как интеллект сети. *Плоскость данных [data plane]* передает сетевой пользовательский трафик. В среде 802.11, эти три логические плоскости работы функционируют по разному в зависимости от типа архитектуры БЛВС и производителя БЛВС. В Главе 11 "Архитектура БЛВС" вы узнаете о прогрессе в развитии корпоративной архитектуры БЛВС и где эти три логические плоскости работают.

## Основы Связи

Хотя сертификация CWNA считается одной из сертификаций начального уровня в программе беспроводной сертификации Сертифицированный Беспроводной Сетевой Профессионал [Certified Wireless Network Professional (CWNP)], это не означает начального уровня сертификации в компьютерной отрасли. Большинство кандидатов на сертификацию CWNA имеют опыт в других областях информационных технологий. Однако, кругозор и опыт этих кандидатов сильно отличается.

В отличие от профессий, для которых знание и экспертиза приобретаются годами структурированного обучения, большинство компьютерных профессионалов идут своим собственным путем образования и тренингов.

Когда люди отвечают за свое собственное образование, они обычно получают те навыки и знания, которые прямо связаны с их интересами или работой. Более фундаментальные знания часто игнорируются, потому что они прямо не относятся к решаемым задачам. Позже, когда их знания увеличиваются и когда они становятся более технически опытными, люди осознают, что им необходимо узнать некоторые основы.

Многие люди в компьютерной индустрии понимают, что при передаче данных, биты передаются по проводам или с помощью радиоволн. Они даже понимают, что используется некоторый тип изменения напряжения или волновых колебаний, чтобы различать биты. Однако, если копнуть по глубже, то у многих из этих людей даже нет идеи о том, что в действительности происходит с электрическими сигналами или волнами.

Следующие разделы дают обзор некоторых фундаментальных принципов связи, которые прямо или косвенно относятся к беспроводной связи. Понимание этих концепций поможет вам лучше понять, что происходит в беспроводной связи, и более просто узнавать и идентифицировать термины, используемые в профессии.

## Терминология Связи

Теперь приведем обзор нескольких базовых сетевых терминов, которые часто неправильно понимаются: **симплекс** [*simplex*], **полудуплекс** [*half-duplex*], и **полный дуплекс** [*full-duplex*]. Есть три способа ведения диалога, которые используются для общения между людьми, а также между вычислительным оборудованием.

**Симплекс [Simplex]** В симплексной связи одно устройство может только передавать, а другое устройство может только принимать. Пример симплексной связи - это FM радио. Симплексная связь редко используется в компьютерных сетях.

**Полу-Дуплекс [Half-Duplex]** В полу-дуплексной связи оба устройства могут передавать и принимать; однако, только одно устройство может передавать одновременно. Пример полудуплексных устройств - рация типа "Уоки-Токи" или обычная рация. Вся радиосвязь по природе является полу-дуплексной, хотя исследования Стэнфордского Университета [Stanford University] гласят, что для приемопередатчиков, способных устранять собственную интерференцию, возможна полнодуплексная связь. Беспроводные сети IEEE 802.11 используют полудуплексную связь.

**Полный Дуплекс [Full-Duplex]** В полнодуплексной связи оба устройства могут передавать и принимать одновременно. Телефонный разговор является примером полнодуплексной связи. Большая часть оборудования IEEE 802.3 поддерживает полнодуплексную связь. На текущий момент, единственный способ осуществлять полнодуплексную связь в беспроводной среде - это наличие двухканальной двунаправленной установки, когда все передачи на одном канале передаются от устройства A к устройству B, а все передачи по другому каналу принимаются устройством A от устройства B. Устройства A и устройства B используют два отдельных радиомодуля на разных каналах.

## Понимание Несущих Сигналов

Так как данные в конечном счете состоят из битов, передатчику нужен способ передачи нулей (0) и единиц (1), чтобы передать данные из одного места в другое. Сигналы переменного (AC) или постоянного (DC) тока сами по себе не выполняют эту задачу. Однако, если сигнал колеблется или изменяется, даже слегка, то сигнал можно интерпретировать так, что данные могут быть отправлены и получены правильно. Этот модифицированный сигнал теперь способен различать между нулями (0) и единицами (1), и называется *несущим сигналом [carrier signal]*. Метод подстройки сигнала для создания несущего сигнала называется *модуляцией [modulation]*.

Три компонента волны, которые могут изменяться или быть изменены, чтобы создать несущий сигнал - это амплитуда, частота и фаза.



Эта глава рассматривает базовые характеристики волн по их отношению к принципам передачи данных. Глава 3 "Основы Радиотехники" рассматривает радиоволны более подробно.

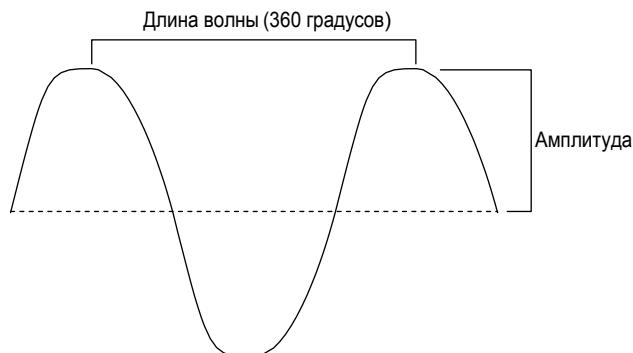
Вся связь на основе радиоволн использует некоторую форму модуляции для передачи данных. Чтобы закодировать данные в сигнал, отправленный АМ/FM радиостанцией, мобильным телефоном, и спутниковым телевидением, над радиосигналом, который передается, производится некоторый тип модуляции. Среднестатистического человека обычно не заботит как сигнал замодулирован, а заботит только то, что устройство работает как надо. Однако, чтобы стать хорошим беспроводным сетевым администратором, вам следует лучше понимать, что в действительности происходит, когда связываются две станции. Оставшаяся часть этой главы приводит вводную часть волны для понимания несущих сигналов и кодирования данных, и представляет вам основы кодирования данных.

## Амплитуда и Длина Волны

Радиосвязь начинается когда радиоволны создаются радиопередатчиком и принимаются, или "слышны", приемником в другом месте. Радиоволны аналогичны волнам, которые вы можете видеть на океане или на озере. Волны состоят из двух главных компонентов: длины волны и амплитуды (см. Рисунок 1.7).

**РИСУНОК 1.7**

## Длина волны и амплитуда волны



**Амплитуда [Amplitude]** Амплитуда [Amplitude] - это высота, сила, или мощность волны. Если бы вы стояли в океане, когда волны приходят на берег, вы бы почувствовали, что сила больших волн намного больше, чем маленьких. Передатчики делают то же самое, но с радиоволнами. Небольшие волны не так заметны, как большие волны. Большие волны генерируют намного больший электрический сигнал, собираемый приемной антенной. Затем приемник может отличить высокие сигналы от низких сигналов.

**Длина волны [Wavelength]** Длина волны [Wavelength] - это расстояние между аналогичными точками на двух волнах, стоящих спина-к-спine. При измерении волны, длина волны обычно измеряется от пика волны до пика следующей волны. Амплитуда и длина волны являются свойствами волн.

## Частота

**Частота [Frequency]** описывает поведение волн. Волны идут от источника, который их генерирует. Как быстро идут волны, или более точно, сколько волн генерируется за период времени в одну секунду, называется частотой [frequency]. Если вы сидели бы на пирсе и считали как часто волны бьют в него, вы могли бы сказать с какой частотой волны приходят на берег. Думайте о радиоволнах таким же образом; однако, радиоволны распространяются намного быстрее, чем волны в океане. Если бы вы попытались сосчитать радиоволны, которые используются в беспроводной связи, то за время, которое нужно для волны воды, чтобы ударить пирс, несколько миллиардов радиоволн также ударили бы пирс.

## Фаза

**Фаза [Phase]** это относительный термин. Это взаимоотношение между двумя волнами с той же самой частотой. Чтобы определить фазу, длину волны делят на 360 частей, называемых градусами [degrees] (см. Рисунок 1.8). Если вы подумаете об этих градусах как о времени старта, то если одна волна начинается с точки в 0-градусов, а другая волна с точки 90-градусов, то считается, что эти волны не в фазе и со сдвигом фазы в 90 градусов.

В идеальном мире волны создавались бы и передавались бы от одной станции и принимались бы идеально в тант на другой станции. К сожалению, радиосвязь происходит в не идеальном мире.

**Р И С У Н О К 1 . 8** Две волны, которые идентичны, но с отличием по фазе в 90 градусов друг относительно друга.



Существует много источников интерференции и множество препятствий, который негативно влияют на волны при их путешествии к принимающей станции. Глава 3 знакомит вас с некоторыми внешними влияниями, которые могут повлиять на целостность волн и вашу возможность общаться между двумя станциями.

### Время и Фаза

Предположим у вас есть двое остановившихся часов, и оба установлены на полдень. В полдень вы запускаете первые часы, а затем запускаете вторые часы часом позже. Вторые часы отстают на один час от первых часов. По мере того как идет время, ваши вторые часы продолжают отставать на один час. Оба часа проработают 24-часовые сутки, но будут не синхронизованы друг с другом. Волны, которые находятся не в фазе ведут себя подобным образом. Две волны, которые находятся не в фазе, фактически, являются двумя волнами, стартовавшими в два разных момента времени. Обе волны совершают полный 360 градусный цикл, но они останутся не в фазе, или не синхронизованными друг с другом.

## Понимание Методов Кодирования

Когда данные отправлены, сигнал передается из приемопередатчика [transceiver]. Для того, чтобы данные были переданы, сигнал должен быть манипулированным таким образом, чтобы принимающая станция имела способ различать нули (0) и единицы (1). Этот метод манипулирования сигнала таким образом, чтобы он мог представлять несколько частей данных, называется методом кодирования [*keying method*]. Метод кодирования – это то, что преобразует сигнал в несущий сигнал. Он обеспечивает сигнал возможностью закодировать данные так, что они могут быть сообщены или транспортированы.

В следующих разделах рассматриваются три типа методов кодирования: кодирование изменением амплитуды или, более принятое название, амплитудная модуляция [amplitude-shift keying (ASK)], кодирование изменением частоты или частотная модуляция [frequency-shift keying (FSK)], и кодирование изменением фазы или фазовая модуляция [phase-shift keying (PSK)]. Эти методы кодирования также называются методами

модуляции [*modulation techniques*]. Методы кодирования используют следующие две разные техники, чтобы представить данные:

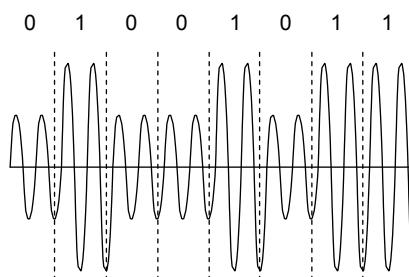
**Текущее Состояние [Current State]** В методе текущего состояния текущая величина (текущее состояние) сигнала используется для различия между нулями (0) и единицами (1). Методы текущего состояния определяют определенную или текущую величину, чтобы обозначить двоичный 0, а другую величину, чтобы обозначить двоичную 1. В определенный момент времени, это та величина, которая определяет двоичное значение. Например, вы можете представить нули и единицы с помощью обычной двери. Раз в минуту вы можете проверять открыта ли дверь или закрыта. Если дверь открыта, то это означает 0, а если дверь закрыта, то это означает 1. Текущее состояние двери в определенное время, открыта или закрыта, это то что определяет нули или единицы.

**Переходное Состояние [State Transition]** В методе переходного состояния используется изменение (или переход из одного состояния в другое) сигнала, чтобы делать различия между нулями и единицами. Методы переходного состояния могут представить 0 изменением в фазе волны в определенное время, а 1 будет представлена отсутствием изменений в фазе волны в определенное время. В определенный момент времени, наличие изменения или отсутствие изменения определяет двоичное значение. В предстоящем разделе “Фазовая Модуляция” приводятся примеры этого подробнее, но дверь можно использовать снова, чтобы привести простой пример. Раз в минуту вы проверяете дверь. В этом случае, если дверь находится в движении (открывается или закрывается), это означает 0, а если дверь покойится (открыта или закрыта), то это означает 1. В этом примере, состояние перехода в определенное время (двигается или не двигается) определяет нули или единицы.

## Амплитудная Модуляция

*Амплитудная модуляция* или *Кодирование Изменением Амплитуды [Amplitude-shift keying (ASK)]* изменяет амплитуду, или высоту сигнала, чтобы представить двоичные данные. ASK – это метод текущего состояния, где один уровень амплитуды может представлять бит со значением 0, а другой уровень амплитуды может представлять бит со значением 1. Рисунок 1.9 показывает, как волна может замодулировать букву K ASCII кода с помощью амплитудной модуляции [amplitude-shift keying]. Волна с большой амплитудой интерпретируется как двоичная (или бинарная) 1, а волна с меньшей амплитудой интерпретируется как двоичный 0.

**Р И С У Н О К 1 . 9** Пример амплитудной модуляции ( Код ASCII заглавной буквы K)



Это переключение амплитуды определяет данные, которые передаются. Способ которым приемная станция выполняет эту задачу заключается в том, чтобы сначала разделить принятый сигнал на периоды времени, которые называются *символьными периодами [symbol periods]*. Принимающая станция затем сравнивает с шаблоном или проверяет волну в течении этого символьного периода, чтобы определить амплитуду волны. В зависимости от величины амплитуды волны, принимающая станция может определить двоичное значение.

Как вы позже узнаете из этой книги, беспроводные сигналы могут быть непредсказуемы, а также подвергаться интерференции от многих источников. Когда происходит зашумление или интерференция, это обычно влияет на амплитуду сигнала. Так как изменение амплитуды из-за шума может привести принимающую станцию к не правильной интерпретации значения данных, ASK стоит использовать с осторожностью.

## Частотная Модуляция

*Частотная модуляция или Кодирование Изменением Частоты [Frequency-shift keying (FSK)]* изменяет частоту сигнала, чтобы представить двоичные данные. FSK это метод текущего состояния, где одна частота может означать бит со значением 0, а другая частота бит со значением 1. (см. Рисунок 1.10). Эта смена частоты определяет данные, которые передаются. Когда приемная станция проводит анализ сигнала во время символьного периода, она определяет частоту волны, и в зависимости от величины частоты, станция может определить двоичное значение.

**РИСУНОК 1.10** Пример частотной модуляции (Код ASCII заглавной буквы K)

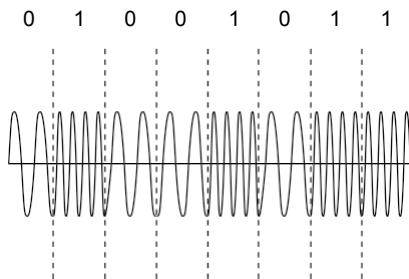


Рисунок 1.10 показывает, как волна может замодулировать букву K ASCII кода с помощью частотной модуляции. Волна с более быстрой частотой представляет двоичную 1, а волна с более медленной частотой представляет двоичный 0.

FSK используется в некоторых устаревших установках беспроводных сетей 802.11. Для более быстрой связи, методы FSK требуют более дорогую технологию, чтобы поддерживать более быстрые скорости, что делает их менее практическими.

### Почему я раньше не слышал о Методах Кодирования?

Вы могли не осознавать этого, но вы слышали о методах кодирования раньше.

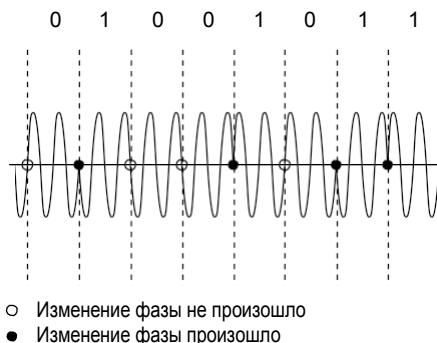
Радиостанции AM/FM используют амплитудную модуляцию (AM) и частотную модуляцию (FM) для передачи сигналов радиостанции, которые вы слушаете дома или в автомобиле.

Радиостанция модулирует голос и музыку в сигнал передачи, а ваша домашняя или автомобильная радиостанция демодулирует его.

## Фазовая Модуляция

*Фазовая модуляция или Кодирование Изменением Фазы [Phase-shift keying (PSK)]* изменяет фазу сигнала, чтобы представить двоичные данные. PSK может быть методом переходного состояния, где изменение фазы может обозначать бит со значением 0, а отсутствие изменения фазы может означать бит со значением 1, или наоборот. Эта смена фазы определяет данные, которые передаются. PSK также может быть методом текущего состояния, где значение фазы может представлять бит «0» или бит «1». Когда принимающая станция анализирует сигнал в течении символьного периода, она определяет фазу волны и статус бита. Рисунок 1.11 показывает, как волна может замодулировать букву K ASCII кода с помощью фазовой модуляции. Изменение фазы в начале символьного периода интерпретируется как двоичная 1, а отсутствие изменения фазы в начале символьного периода интерпретируется как двоичный 0.

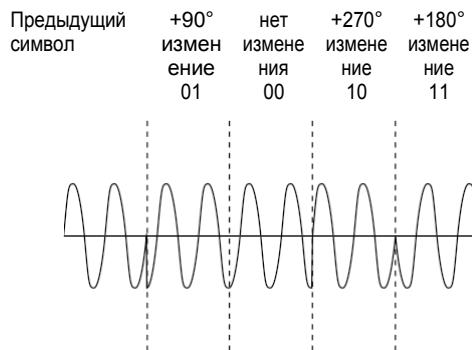
**Р И С У Н О К 1.11** Пример фазовой модуляции (Код ASCII заглавной буквы K)



Технология PSK активно используется для радиопередач в соответствии со стандартом 802.11- 2020. Обычно, принимающая станция анализирует сигнал в течении символьного периода, сравнивает фазы текущего образца с предыдущим образцом, и определяет разницу. Эта степень (или градус) разницы, или *дифференциал [differential]*, используется для определения значения бита.

Более продвинутые версии PSK могут кодировать несколько битов на символ. Вместо использования двух фаз, чтобы представлять двоичные значения, вы можете использовать четыре фазы. Каждая из четырех фаз способна представлять два двоичных значения (00, 01, 10, или 11), вместо одного (0 или 1), таким образом сокращая время общей передачи. Когда используется более двух фаз, то это называется *многофазной модуляцией* или *кодированием с множеством смен фаз [multiple phase-shift keying (MPSK)]*. Рисунок 1.12 показывает, как волна может замодулировать букву K кода ASCII с помощью метода MPSK. Можно отследить четыре возможных изменения фазы, каждое изменение фазы теперь можно интерпретировать как 2 бита данных вместо 1. Заметьте, что на этом рисунке символьное время меньше, чем на Рисунке 1.10.

**РИСУНОК 1.12** Пример многофазной модуляции (Код ASCII заглавной буквы *K*)



### Где Можно Узнать Больше о Технологии 802.11 и Wi-Fi Отрасли?

Чтение этой книги от корки до корки – это огромный путь для начала понимания технологии Wi-Fi. Из-за быстро меняющейся природы технологий БЛВС 802.11, авторы этой книги рекомендуют следить за дополнительными ресурсами:

**Wi-Fi Альянс** Как ранее упоминалось, Wi-Fi Альянс – это маркетинговый голос Wi-Fi отрасли, и управляет всеми отраслевыми сертификациями. Вебсайт Wi-Fi Альянса, [www.wi-fi.org](http://www.wi-fi.org), является замечательным ресурсом.

**CWNP** Программа Сертифицированный Беспроводной Сетевой Профессионал [Certified Wireless Networking Professional] управляет образовательными ресурсами, включая форумы пользователей и базу данных информационных бюллетеней о БЛВС [WLAN white paper]. Вебсайт, [www.cwnp.com](http://www.cwnp.com), также является лучшим источником информации обо всех нейтральных к производителям сертификациям по беспроводным сетям по программе CWNP.

**Вебсайты Производителей БЛВС** Хотя экзамен CWNA и эта книга используют нейтральный к производителям подход в обучении 802.11, вебсайты различных производителей БЛВС часто являются прекрасными ресурсами информации по определенным решениям Wi-Fi сети. Многие основные производители БЛВС упоминаются в этой книге, а список вебсайтов большинства основных производителей БЛВС можно найти в Главе 20 “Установка БЛВС и Вертикальные Рынки”.

**Wi-Fi Блоги** В последние годы многочисленные персональные блоги по теме Wi-Fi внезапно заполонили весь Интернет. Большой пример блога, написанного CWNE #135 Найджелом Боуденом [Nigel Bowden],

<https://wifinigel.blogspot.com>

Еще один прекрасный блог - это Wirednot blog (\*Непроводной блог), написанный Wi-Fi экспертом Ли Бэдменом [Lee Badman], CWNE #200,

<https://wirednot.wordpress.com>

Глен Кейт [Glenn Cate], CWNE #181, поддерживает огромный список Wi-Fi блогов с ссылками на большинство коммерческих и персональных блогов об индустрии БЛВС

<https://gcatewifi.wordpress.com>

**Wi-Fi Подкасты** Технические подкасты чрезвычайно популярны у IT профessionалов, кто ездит на работу каждый день. А там представлен широкий ассортимент толковых подкастов, которые сосредоточены на Wi-Fi. Самый долгий и наиболее прослушиваемый Wi-Fi подкаст ведется Кейтом Парсонсом [Keith Parsons], CWNE #3. Подкаст Профессионалов Беспроводных ЛВС [wirelessLAN Professionals] великий ресурс для любого, кто хочет узнать о Wi-Fi.

<https://wanprofessionals.com/podcast>

Роуэлл Дионисио [Rowell Dionicio] CWNE #210 и Франсуа Верже [François Vergès] CWNE #189, ведут подкаст Clear To Send [Готов к Передаче] о беспроводной инженерии. Они делятся полезными советами и ресурсами, и обсуждают темы о беспроводной связи с также мыслящими людьми.

[www.cleartosend.net](http://www.cleartosend.net)

Мак Деринг [Mac Deryng] CWNE #357, и Мэтт Старлинг [Matt Starling] CWNE #369, выпускают подкаст Wi-Fi Нинзя [Wi-Fi Ninjas]. Их подкаст сфокусирован на проектирование, установку и обследование Wi-Fi, а также на RTLS.

<https://wifininjas.net>

**Технические Конференции про Wi-Fi** Различные организации предлагают технические конференции, которые относятся к отрасли БЛВС. Безусловно самая популярная техническая конференция по Wi-Fi - это Конференция Профессионалов Беспроводных ЛВС [the wirelessLAN Professionals Conference], проводимая несколько раз в год в разных регионах мира. Все презентации выступающих также становятся доступными бесплатно после конференции. Вы можете узнать больше о Конференции Профессионалов Беспроводных ЛВС [wirelessLAN Professionals Conference] по адресу

[www.wlanpros.com](http://www.wlanpros.com)

Вы ищите хорошую конференцию сосредоточенную на бизнесе Wi-Fi? Тогда попробуйте посетить одну из конференций Wi-Fi Сейчас [Wi-Fi NOW]. Wi-Fi NOW организует ежегодные мероприятия Wi-Fi отрасли в Соединенных Штатах, Европе и Азии. Больше информации находится на сайте

<https://wifinowglobal.com>

\*Указанные ранее конференции - это, как правило, конференции на английском языке. Стоит отметить, что в России под эгидой компании CompTek проводилась ежегодная конференция посвященная беспроводной связи с названием Беседа. Но последние несколько лет конференция не проводится. Надеюсь, что конференция снова начнет проводится на ежегодной основе. Больше узнать о конференции Беседа и ознакомиться с материалами можно по адресу

<http://beseda.ru/22/>

**Slack** Существует много мест где Wi-Fi люди зависают и общаются на специфичные темы. Slack группа Wi-Fi Pros - это одно из таких мест, где вы можете что-нибудь узнать, поделиться и сделать вклад в Wi-Fi сообщество. Вы можете запросить приглашение в этот канал через [admin@thewifiprosslack.com](mailto:admin@thewifiprosslack.com) или через Twitter через администраторов: Mae Лессард [Mae Lessard] (@Mae149), Сэм Клементс [Sam Clements] (@samuel\_clements), и Фил Морган [Phil Morgan] (@CCIE5224). Обратите внимание, что эта группа не аффилирована ни с каким производителем.

**Twitter** Техническое сообщество БЛВС очень активно в Twitter. Эксперты Wi-Fi отрасли используют платформы социальных сетей как способ публичного общения и способом поделиться информацией. Вы можете следовать за авторами этой книги Дэвидом Коулменом [David Coleman] и Дэвидом Уэсткоттом [David Westcott] в Twitter: [@mistermultipath](#) и [@davidwestcott](#), соответственно.

\***Telegram** Есть аналогичные каналы или чаты в Telegram. Один из таких русскоязычных чатов по Wi-Fi это Злой Беспроводной Чат

[t.me/EvilWirelessChat](https://t.me/EvilWirelessChat)

# Итого

Эта глава объясняет историю беспроводных сетей, и роли и ответственности следующих ключевых организаций, вовлеченных в отрасль беспроводных сетей:

- FCC и другие государственные регуляторы
- IEEE
- IETF
- Wi-Fi Альянс

Чтобы дать базовое понимание взаимосвязи между сетевыми основами и технологиями 802.11, мы обсудили следующие концепции:

- Модель OSI
- Ядро, распределение, и доступ

Чтобы дать базовые знания о том как беспроводная станция передает и принимает данные, мы познакомили вас с компонентами волн и модуляций:

- Несущие сигналы
- Амплитуда
- Длина волны
- Частота
- Фаза
- Методы кодирования (модуляции), включая ASK, FSK, и PSK

Когда вы решаете проблему радиосвязи, обладание твердыми знаниями о волнах и методах модуляций может помочь вам понять проблемы, лежащие в основе проблем связи, и поможет привести вас к решению.

# Темы Экзамена

**Знать четыре отраслевые организации.** Понимать роли и ответственности государственных регулирующих организаций, IEEE, IETF, и Wi-Fi Альянс.

**Понимать что такое ядро, распределение и доступ.** Знать где устанавливается технология 802.11 в фундаментальном сетевом проекте (дизайне).

**Объяснить разницу между симплексной, полу duplexной и полнодуплексной связью.** Знать, что радиосвязь, включая радиосвязь 802.11, является полу duplexной.

**Понимать что такое длина волны, частота и фаза.** Знать определения каждой радиохарактеристики.

**Понимать концепцию модуляции.** ASK, FSK, и PSK являются тремя методами модуляции несущего сигнала.

# Контрольные Вопросы

1. Технология 802.11 обычно применяется на каком фундаментальном уровне сетевой архитектуры?
  - A. Уровне ядра [Core]
  - B. Уровне распределения [Distribution]
  - C. Уровне доступа [Access]
  - D. Сетевом уровне [Network]
2. Какая организация ответственна за применение правил по максимальной мощности передачи в нелицензируемой полосе частот?
  - A. IEEE
  - B. Wi-Fi Альянс
  - C. ISO
  - D. IETF
  - E. Ни одна из выше перечисленных
3. Беспроводной мост 802.11 обычно ассоциируется с каким уровнем сетевой архитектуры?
  - A. Уровнем ядра [Core]
  - B. Уровнем распределения [Distribution]
  - C. Уровнем доступа [Access]
  - D. Сетевым уровнем [Network]
4. Стандарт 802.11-2020 был создан какой организацией?
  - A. IEEE
  - B. OSI
  - C. ISO
  - D. Wi-Fi Альянс
  - E. FCC
5. Какая организация обеспечивает совместимость продукции БЛВС?
  - A. IEEE
  - B. ITU-R
  - C. ISO
  - D. Wi-Fi Альянс
  - E. FCC
6. Какой тип сигнала требуется для передачи данных?
  - A. Сигнала связи
  - B. Сигнала данных

- C.** Несущий сигнал
  - D.** Двоичный сигнал
  - E.** Цифровой сигнал
7. Какой метод кодирования наиболее восприимчив к интерференции от шума?
- A.** FSK
  - B.** ASK
  - C.** PSK
  - D.** DSK
8. Какой подуровень модели Канального [Data-Link] уровня модели OSI используется для связи между радиомодулями 802.11?
- A.** LLC
  - B.** PLCP
  - C.** MAC
  - D.** PMD
9. При проведении некоторых изысканий Джени пришла к ссылке на документ с названием RFC 3935. Вебсайт какой из следующих организаций лучше всего подходит для дальнейшего исследования этого документа?
- A.** IEEE
  - B.** Wi-Fi Альянс
  - C.** WECA
  - D.** FCC
  - E.** IETF
10. Какие три логические плоскости работы сетей связи?
- A.** Плоскость управления [Management]
  - B.** Плоскость ядра [Core]
  - C.** Плоскость контроля [Control]
  - D.** Плоскость доступа [Access]
  - E.** Плоскость данных [Data]
11. Какие свойства волны могут быть модулированы, чтобы закодировать данные? (Выберите все, что применимо.)
- A.** Амплитуда
  - B.** Частота
  - C.** Фаза
  - D.** Длина волны

- 12.** Стандарт IEEE 802.11-2020 определяет механизмы связи на каких уровнях модули OSI? (Выберите все, что применимо.)
- A.** Сетевом [Network]
  - B.** Физическом [Physical]
  - C.** Транспортном [Transport]
  - D.** Прикладном [Application]
  - E.** Канальном [Data-Link]
  - F.** Сеансовом [Session]
- 13.** Высота или мощность волны называется как ... ?
- A.** Фаза
  - B.** Частота
  - C.** Амплитуда
  - D.** Длина волны
- 14.** СЕРТИФИЦИРОВАННЫЙ Wi-Fi 6 [Wi-Fi CERTIFIED 6] сертифицирует работу и возможности какого беспроводного стандарта 802.11? (Выберите все, что применимо.)
- A.** 802.11ac
  - B.** 802.11ax
  - C.** 802.1X
  - D.** 802.11ay
- 15.** За что из нижеперечисленного отвечает Подразделение Инженерных Задач Интернета [Internet Engineering Task Force (IETF)]?
- A.** Запрос Комментариев [Request for Comments (RFCs)]
  - B.** Стандарты 802.11
  - C.** Стандарты СЕРТИФИЦИРОВАННЫЙ Wi-Fi [Wi-Fi CERTIFIED]
  - D.** Правила официальной организации определенного регуляторного региона.
- 16.** Какие из следующих параметров беспроводной связи и типов использования обычно управляются местным регулирующим органом? (Выберите все, что применимо.)
- A.** Частота [Frequency]
  - B.** Ширина полосы [Bandwidth]
  - C.** Максимальная мощность передачи [Maximum transmit power]
  - D.** Максимальная ЭИИМ [EIRP]
  - E.** Использование внутри/снаружи помещений
- 17.** Какой тип связи используют радиомодули 802.11 для передачи и приема?
- A.** Симплексный [Simplex]
  - B.** Полудуплексный [Half-duplex]
  - C.** Полнодуплексный [Full-duplex]
  - D.** Эходуплексный [Echo-duplex]

### Контрольные Вопросы

- 18.** Волна поделена на градусы. Сколько градусов образуют полную волну?
- A.** 100
  - B.** 180
  - C.** 212
  - D.** 360
- 19.** Какие преимущества использования нелицензируемых полос частот для радиопередач?  
(Выберите все, что применимо.)
- A.** Нет государственного регулирования.
  - B.** Нет дополнительных финансовых затрат.
  - C.** Любой может использовать полосу частот.
  - D.** Нет правил.
- 20.** Модель OSI состоит из скольких уровней?
- A.** Четырех
  - B.** Шести
  - C.** Семи
  - D.** Девяти



# Глава 2



## Стандарт и Поправки IEEE 802.11

---

**В ЭТОЙ ГЛАВЕ ВЫ УЗНАЕТЕ О СЛЕДУЮЩЕМ:**

✓ **Первоначальный стандарт IEEE 802.11**

- IEEE 802.11-2020, принятые поправки
- 802.11a-1999
- 802.11b-1999
- 802.11d-2001
- 802.11e-2005
- 802.11g-2003
- 802.11h-2003
- 802.11i-2004
- 802.11j-2004
- 802.11k-2008
- 802.11n-2009
- 802.11p-2010
- 802.11r-2008
- 802.11s-2011
- 802.11u-2011
- 802.11v-2011
- 802.11w-2009
- 802.11y-2008
- 802.11z-2010
- 802.11aa-2012
- 802.11ac-2013
- 802.11ad-2012



- 802.11ae-2012
- 802.11af-2014
- 802.11ah-2016
- 802.11ai-2016
- 802.11aj-2018
- 802.11ak-2018
- 802.11aq-2018

✓ **IEEE 802.11, черновые поправки**

- 802.11ax
- 802.11ay
- 802.11az
- 802.11ba
- 802.11bb
- 802.11bc
- 802.11bd
- 802.11be

✓ **Нерабочие Поправки**

- 802.11F
- 802.11T

✓ **IEEE Группа по Задаче m**



Как обсуждалось в Главе 1 “Обзор Беспроводных Стандартов, Организаций и Основ”, Институт Инженеров Электротехники и Электроники [Institute of Electrical and Electronics Engineers (IEEE)] является профессиональным сообществом, которое создает и управляет стандартами,

которые мы используем для связи, такие как стандарт 802.3 Ethernet для проводных сетей. IEEE назначил рабочие группы для нескольких беспроводных стандартов связи. Например, рабочая группа 802.15 отвечает за связь в сети персональной зоны действия [personal area network (PAN)], использующей радиочастоты, например, Bluetooth. Еще один пример – это стандарт 802.16, за которым следит рабочая группа по Стандартам Широкополосного Беспроводного Доступа [Broadband Wireless Access Standards]; эта технология часто называется, как WiMAX. Эта книга сосредоточена на технологии, определенной стандартом IEEE 802.11, который обеспечивает связь для локальной вычислительной сети, использующей радиочастоты.

Рабочая группа 802.11 имеет около 400 активных членов из более чем 200 беспроводных компаний. Она состоит из постоянных комитетов, исследовательских групп, и многочисленных групп по задачам [*task groups*]. Например, Постоянный Комитет по Публичности [Standing Committee—Publicity (PSC)] отвечает за нахождение средств, чтобы лучше рекламировать стандарт 802.11. Исследовательская Группа 802.11 [802.11 Study Group (SG)] одобряется исполнительным комитетом [*executive committee (EC)*], и ожидается, что будет иметь короткий срок жизни, обычно меньше шести месяцев. Исследовательская группа отвечает за исследование возможности внедрения новых характеристик и возможностей в стандарт 802.11.

## IEEE 802.11: Больше о Рабочей Группе и Стандарте 2020

Вы можете найти краткое руководство рабочей группы IEEE 802.11

[www.ieee802.org/11/QuickGuide\\_IEEE\\_802\\_WG\\_and\\_Activities.htm](http://www.ieee802.org/11/QuickGuide_IEEE_802_WG_and_Activities.htm)

Стандарт 802.11-2020 и принятые поправки доступны по адресу

<https://ieeexplore.ieee.org/browse/standards/get-program/page>

Некоторые из стандартов и документов принятых поправок являются бесплатными, а другие (особенно недавно принятые документы) доступны за плату.

Различные группы по задачам 802.11 отвечают за пересмотр и исправление исходных стандартов, которые были разработаны группой по задаче MAC [MAC task group (MAC)] и группой по задаче PHY [PHY task group (PHY)]. Каждой группе назначается буква из алфавита, и это нормально слышать термин 802.11 алфавитный винегрет [802.11 *alphabet soup*], когда ссылаются на все поправки, созданные несколькими группами по задачам 802.11.

Когда группы по задачам сформированы, им назначается следующая по списку доступная буква по алфавиту, хотя поправки могут быть принятами не обязательно в том же самом порядке. Довольно много проектов групп по задачам 802.11 были завершены, и поправки к первоначальному стандарту были приняты. Проекты других групп по задачам 802.11 все еще активны и существуют в качестве черновых поправок.

В этой главе мы обсуждаем первоначальный стандарт 802.11, принятые поправки (многие из которых были включены в стандарт 802.11-2007, стандарт 802.11-2012, стандарт 802.11-2016, и текущий стандарт 802.11-2020), и черновые поправки различных групп по задачам 802.11.

## Первоначальный Стандарт IEEE 802.11

Исходный стандарт 802.11 был опубликован в Июне 1997 года как IEEE Std 802.11-1997, и часто называется, как 802.11 Исходный [802.11 Prime], потому что он был первым стандартом БЛВС. Стандарт был пересмотрен в 1999 году, переутверждён в 2003 году, и опубликован как IEEE Std 802.11-1999 (R2003). 8ого марта 2007 года еще одна итерация стандарта была утверждена IEEE Std 802.11-2007, 29 марта 2012 года был утвержден стандарт IEEE Std 802.11-2012, а 7ого декабря 2016 года был утвержден IEEE Std 802.11-2016. Самая последняя версия стандарта - это IEEE 802.11-2020, который был утвержден в декабре 2020 года.

IEEE определяет технологии 802.11 только на Физическом уровне и MAC подуровне Канального уровня [Data-Link layer]. По проекту, стандарт 802.11 не рассматривает верхние уровни модели OSI, хотя существует взаимодействие между MAC уровнем 802.11 и более высокими уровнями по таким параметрам, как качество сервиса (QoS). Группа по задаче [task group] PHY (т.е. физического уровня) работала совместно с группой по задаче MAC (т.е. уровня доступа к среде), чтобы определить исходный стандарт 802.11. Рабочая группа по задаче PHY определяла три первоначальных спецификации Физического уровня:

**Инфракрасная связь [Infrared]** Технология инфракрасной связи [*Infrared (IR)*] использует среду на основе луча света. Хотя инфракрасная среда и была в действительности определена в исходном стандарте 802.11, с тех пор она была не рекомендована и убрана из стандарта.

**Расширение Спектра с Перестройкой Частоты [Frequency-Hopping Spread-Spectrum]** Радиоволновые сигналы могут быть определены как узкополосные сигналы или как сигналы расширения спектра. Радиосигнал считается *расширением спектра [spread-spectrum]*, когда ширина полосы пропускания шире, чем это требуется для передачи данных. *Расширение Спектра с Перестройкой Частоты [Frequency-hopping spread-spectrum (FHSS)]* - это технология расширения спектра, которая впервые была запатентована во время Второй Мировой Войны. Перестройка частоты в 802.11 была не рекомендована и убрана из стандарта.

**Расширение Спектра Прямой Последовательности [Direct-Sequence Spread-Spectrum]** *Расширение спектра прямой последовательностью [Direct-sequence spread-spectrum (DSSS)]* - это еще одна технология расширения спектра, которая использует фиксированные каналы. Радиомодули DSSS 802.11 называются устройствами Статьи 15 [Clause 15 devices].

## Что такое Статья IEEE [IEEE Clause]?

Стандарты IEEE являются очень упорядоченными, структурированными документами. Документ стандартов иерархически структурирован, каждый раздел пронумерован (например, как 7.3.2.4). Самый верхний уровень (7) называется, как статья [*clause*], разделы уровней ниже (3.2.4) называются как подстатьи [*subclauses*]. Когда создается поправка, разделы в поправке нумеруются относительно последней версии стандарта, даже если поправка - это отдельный документ. Когда стандарт и его поправки объединяются в новую версию стандарта, как это было сделано с IEEE Std 802.11-2020, статьи и подстатьи всех отдельных документов являются уникальными, что позволяет объединить документы стандарта и поправок без изменения номера какого-либо раздела (статьи/подстатьи). В 2020 году IEEE пересмотрел стандарт снова и объединил в группу пять поправок. Когда эта книга завершалась, IEEE утвердил обновление в декабре 2020 года. Ожидается, что IEEE Std 802.11-2020 будет опубликовано в Феврале 2021 года. Многие годы, когда принимались новые поправки, разным поправкам требовалось больше или меньше времени.

Следовательно, порядок некоторых статей был не в хронологическом порядке. Хотя это не требовалось, некоторые статьи были переставлены и перенумерованы в IEEE Std 802.11-2012 так, чтобы статьи шли в хронологическом порядке, на основе того, когда они были приняты. Кроме консолидации некоторых принятых поправок, IEEE Std 802.11-2016 удалили некоторые устаревшие статьи и переорганизовал некоторые другие. Когда бы мы не ссылались на какую-либо статью в этой книге, мы будем использовать текущую схему нумерации, определенную в пересмотренном стандарте 2016 года, и оставшуюся в стандарте IEEE Std 802.11-2020. Эта книга ссылается на статьи так, чтобы вы знали про них и понимали куда идти, если вы захотите узнать больше о технологии. Обратите внимание, однако, что Вас не будут проверять на знание номеров статей на экзамене CWNA (CWNA-108).

Как определено Исходным 802.11 [802.11 Prime], первоначальное частотное пространство, в котором радиомодулям разрешалось передавать, было не требующее лицензии 2,4 ГГц *промышленной, научной и медицинской* [*industrial, scientific, and medical (ISM)*] полосой. Радиомодули DSSS 802.11 могут передавать внутри каналов, выделенных из всей полосы ISM, от 2.4 ГГц до 2.4835 ГГц. IEEE был более жесток к радиомодулям FHSS, которым было разрешено передавать на 1МГц поднесущих в диапазоне от 2.402 ГГц до 2.480 ГГц полосы ISM 2.4 ГГц.

Вы вероятно никогда не работали с каким-либо устаревшим радиомодулем, определенным в Исходном 802.11 [802.11 Prime], потому что технологии более 20 лет, и она была заменена в работающих средах БЛВС. Изначально, у производителей БЛВС был выбор делать радиомодули FHSS или радиомодули DSSS. Большая часть ранних установок БЛВС использовали частотное перестроение, но было и несколько решений с DSSS. Стоит также отметить, что все ссылки на радиомодули FHSS из текущего стандарта 802.11-2020 устарели.

Что на счет скорости? Скорости передачи данных, определенные исходным стандартом 802.11, были 1 Мбит/с и 2Мбит/с, независимо от того, какая технология расширения спектра использовалась. *Скорость передачи данных [data rate]* - это число битов Физического уровня переносимых за секунду во время передачи, обычно указывается как количество миллионов бит в секунду (Мбит/с). Держите в уме, что скорость передачи данных [data rate] - это *скорость [speed]*, а не реальная *пропускная способность [throughput]*. Из-за методов доступа к среде и служебной информации [overhead] самой связи, агрегированная пропускная способность обычно где-то половина от доступной скорости передачи данных.

## IEEE 802.11-2020, Принятые Поправки

В годы, последовавшие за публикацией исходного стандарта 802.11, были собраны новые рабочие группы по задачам, чтобы работать над потенциальными улучшениями стандарта. За время написания книги почти 30 поправок было принято и опубликовано отдельными рабочими группами по задачам. В 2007 году IEEE объединил восемь принятых поправок вместе с исходным стандартом, создав единый документ, который был опубликован как *IEEE Std 802.11-2007*. Эта ревизия также включала исправления, уточнения и улучшения.

В 2012 году IEEE объединила 10 принятых поправок в стандарт, создав единый документ, который был опубликован как *IEEE Std 802.11-2012*. Кроме объединения принятых поправок и внесения исправлений, уточнений и улучшений в документ, IEEE пересмотрел все статьи и приложения в хронологическом порядке. Некоторые статьи и приложения были переупорядочены и перенумерованы так, чтобы они шли в порядке, в котором они были приняты.

В 2016 году IEEE консолидировал пять принятых поправок в стандарт, создав новый документ, опубликованный как *IEEE Std 802.11-2016*. Кроме объединения принятых поправок и внесения исправлений, некоторые устаревшие статьи были удалены из документа, а некоторые статьи были перенумерованы.

Самое последнее, в 2020 году, IEEE объединил пять принятых поправок в последней редакции стандарта *IEEE Std 802.11-2020*.

### Терминология Экзамена CWNA

В 2020 году IEEE консолидировал стандарт 2016 вместе с принятыми поправками в единый документ, который теперь опубликован как стандарт 802.11-2020. Технически, любая поправка, которая была консолидирована в обновленный стандарт, больше не существует, потому что она объединена в единый документ. Однако, Wi-Fi Альянс и большинство профессионалов БЛВС продолжают ссылаться на принятые поправки по названию.

Ранние версии экзамена CWNA не ссылались ни на одну поправку 802.11 по названию, и проверяли вас только на технологии, используемые каждой поправкой. Например, 802.11b – это принятая поправка, которая является частью стандарта 802.11-2020. Технология, которая изначально была определена поправкой 802.11b, называлась Высоко-Скоростное DSSS [High-Rate DS-SS] (HR-DS-SS). Хотя название 802.11b, фактически, осталось наиболее употребительным термином, более старые версии экзамена CWNA используют только технический термин HR-DS-SS, вместо более употребительного термина, 802.11b.

Текущая версия экзамена CWNA (CWNA-108) использует более употребительную терминологию поправок 802.11, такую как 802.11b.

Вспомните, как вы узнали из Главы 1, Wi-Fi Альянс принял новое соглашение по

наименованиям по поколениям для Wi-Fi технологий. Например, 802.11ax называется, как Wi-Fi 6; 802.11ac можно называть как Wi-Fi 5, а 802.11n как Wi-Fi 4.

Для экзамена CWNA (CWNA-108), вам следует все еще понимать разницу между разными технологиями и тем как они работают. Хорошее понимание того, какая технология какой поправкой определена, будет полезна для вашей карьеры.

## 802.11a-1999

В тот же самый год, когда была утверждена поправка 802.11b, еще одна важная поправка была утверждена также и опубликована как *IEEE Std 802.11a-1999*. Инженеры в Рабочей Группе по Задаче а [Task Group a (TGA)] приступили к определению того, как технологии 802.11 будут работать в 5 ГГц частотном пространстве, используя радиотехнологию, называемую *ортогональное мультиплексирование с частотным разделением* [*orthogonal frequency-division multiplexing (OFDM)*]. Радиомодули 802.11a могли передавать в трех разных 100 МГц нелицензируемых полосах частот в 5 ГГц диапазоне. Эти три полосы называются полосы частот *Нелицензируемой Национальной Информационной Инфраструктуры* [*Unlicensed National Information Infrastructure (U-NII)*]. Всего были доступны 12 каналов в первоначальных трех полосах U-NII. Все аспекты принятой поправки 802.11a теперь могут быть найдены в Статье 17 стандарта 802.11-2020.

Полоса ISM в 2.4 ГГц является намного более переполненным пространством частот, чем полосы U-NII в 5 ГГц. Устройства Bluetooth, микроволновые печи, беспроводные телефоны и многочисленные другие устройства, все работают в полосе ISM 2.4 ГГц, и являются потенциальными источниками интерференции. Кроме того, абсолютное число установок БЛВС 2.4 ГГц является проблемой, особенно в таких средах, как многоофисные здания.

Большое преимущество использования оборудования БЛВС 5 ГГц в том, что полосы U-NII менее загружены. Со временем, три первоначальных полосы U-NII также начнут становиться переполненными. Регулирующие организации такие, как FCC открыли больше частотного пространства в диапазоне 5 ГГц, а IEEE отразил это в поправке 802.11h. FCC также предложила сделать доступным еще больше 5 ГГц спектра в будущем. Существенно больше подробностей обо всех полосах U-NII в 5 ГГц можно найти в Главе 6 “Беспроводные Сети и Технологии Расширения Спектра”.

Устаревшие радиомодули 802.11a вначале могли передавать по 12 каналам полос U-NII-1, U-NII-2, и U-NII-3; однако, 5 ГГц частотный диапазон и каналы, используемые радиомодулями 802.11a зависят от регулирующего радиочастоты органа каждой страны. Поправка в основном была про введение технологии OFDM, которая предоставляет более лучшие, более высокие скорости



Вы найдете больше обсуждений о полосах ISM и U-NII в Главе 6.

Радиомодули 802.11a, работающие в полосах 5 ГГц U-NII классифицируются как *устройства Статьи 17* [*Clause 17 devices*]. Как определено поправкой 802.11a, эти устройства требуются для поддержки скорости передачи данных в 6, 12, и 24 Мбит/с, с максимумом в 54 Мбит/с. При использовании технологии, которая называется ортогональное мультиплексирование с разделением частоты [*orthogonal frequency-division multiplexing (OFDM)*], поддерживаются скорости передачи данных в 6, 9, 12, 18, 24, 36, 48, и 54 Мбит/с. OFDM также обсуждается в Главе 6.

Стоит отметить, что радиомодули 802.11a не могут связываться с устаревшими радиомодулями 802.11, 802.11b или 802.11g по двум причинам. Первое, радиомодули 802.11a используют другую радиотехнологию, нежели чем устаревшие 802.11 или 802.11b устройства. Второе, устройства 802.11a передают в полосах 5 ГГц U-NII, в то время как устройства 802.11/802.11b/802.11g работают в полосе 2,4 ГГц ISM. Хорошая новость в том, что 802.11a может сосуществовать в том же физическом пространстве с 802.11, 802.11b, или 802.11g устройствами, потому что они передают в отдельных частотных диапазонах.

Когда 802.11a был впервые принят, ушло почти два года прежде, чем устройства стали легко доступными. Когда устройства 802.11a стали доступными, чипсеты радиомодулей, использующие OFDM были достаточно дорогими. Из-за этих двух факторов, широко развернутые БЛВС 5 ГГц на предприятиях были редкими. В конце концов чипсеты стали доступными, и использование полос частот 5 ГГц значительно выросло с годами. Производители БЛВС разработали двух частотные точки доступа (ТД) с радиомодулями 2,4 ГГц и 5 ГГц. Большинство ноутбуков, произведенных с 2007 года, поддерживают двухчастотные радиомодули. В большинстве установок беспроводных сетей на предприятиях работает 2,4 ГГц и 5 ГГц беспроводные сети 802.11 одновременно, при этом 5 ГГц сеть более предпочтительна.

## **802.11b-1999**

Хотя потребительский рынок Wi-Fi продолжал расти с огромной скоростью, 802.11b-совместимое оборудование БЛВС дало отрасли первый необходимый большой толчок. В 1999 году IEEE Группа по Задаче b [IEEE Task Group b (TGb)] опубликовала IEEE Std 802.11b-1999, который позже был поправлен и скорректирован как IEEE Std 802.11b-1999/Cor1-2001. Все аспекты принятой поправки 802.11b теперь можно найти в Статье 16 стандарта 802.11-2020.

Среда Физического уровня, которая была определена 802.11b - это *Высоко-Скоростное DSSS [High-Rate DSSS (HR-DSSS)]*. Частотное пространство, в котором радиокарты 802.11b могут работать - это нелицензируемая полоса от 2,4 ГГц до 2,4835 ГГц.

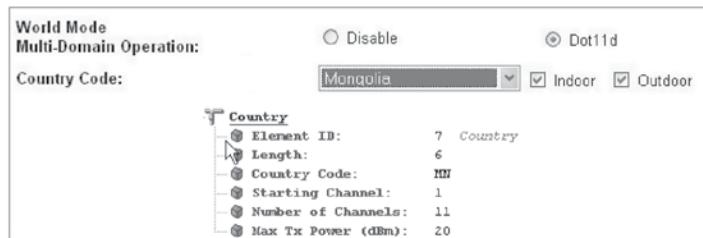
Главная цель Группы по Задаче b (TGb) была в достижении высоких скоростей передачи данных в полосе 2,4 ГГц ISM. Радиоустройства 802.11b выполнили этот геройский поступок с помощью другой техники расширения/кодирования, с названием *модуляция дополнительным кодом или кодирование с дополнительным кодом [complementary code keying (CCK)]*, и методами модуляции, использующими свойства фазы радиосигнала. Устройства 802.11 использовали технику расширения, называемую *код Баркера [Barker code]*. Конечный результат в том, что радиоустройства 802.11b поддерживают скорости передачи данных в 1, 2, 5,5, и 11 Мбит/с. Системы 802.11b обратно совместимы со скоростями передачи данных 802.11 DSSS в 1 Мбит/с и 2 Мбит/с. Скорость передачи данных в 5,5 Мбит/с и 11 Мбит/с называется HR-DSSS. Еще раз, нужно понимать, что поддерживаемые скорости передачи данных относятся к скорости передачи, а не к агрегированной пропускной способности. Радиомодули 802.11b не были обратно совместимыми с устаревшими радиомодулями 802.11 FHSS, потому что разные технологии расширения спектра не могут взаимодействовать друг с другом. Опциональная технология, с названием *Пакетное Двоичное Сверточное кодирование [Packet Binary Convolutional coding (PBCC)]* было убрано из стандарта IEEE.

## 802.11d-2001

Исходный стандарт 802.11 был написан для соответствия регуляторной области Соединенных Штатов, Японии, Канады и Европы. Регуляторы в других странах могли определить другие ограничения на разрешенные частоты и мощность передачи. Поправка 802.11d, которая была опубликована как IEEE Std 802.11d-2001, добавила требования и определения, необходимые для возможности оборудованию БЛВС 802.11 работать в областях, не обслуживаемых оригинальным стандартом.

Информация о коде страны предоставляется в полях внутри двух беспроводных кадров, которые называются маяки [*beacons*] и зондирующие ответы или ответы на зондирующие запросы [*probe responses*]. Эта информация затем используется 802.11d-совместимыми устройствами для удостоверения, что они следуют частотным и мощностным правилам определенной страны. Рисунок 2.1 показывает ТД, настроенную для использования в Монголии, и перехваченные кадр маяка [*beacon frame*], содержащий информацию о коде страны, частоте и мощности.

**РИСУНОК 2.1** Настройки 802.11d



Все аспекты принятой поправки 802.11d теперь можно найти в стандарте 802.11-2020.



Подробное обсуждение маяков [*beacons*], зондов [*probes*], и других беспроводных кадров можно найти в Главе 9 “802.11 MAC.”

## 802.11e-2005

Исходный стандарт 802.11 не определял процедуры качества сервиса [*quality of service (QoS)*] для использования приложений чувствительных ко времени таких, как Голос через Wi-Fi [*Voice over Wi-Fi*]. Голос по Wi-Fi [*Voice over Wi-Fi*] также называется, как Голос через Беспроводную ЛВС [*Voice over Wireless LAN (VoWLAN)*]. Терминология, используемая многими производителями и программой CWNP, - это Голос через Wi-Fi [*Voice over Wi-Fi (VoWiFi)*]. Трафик Приложений таких, как голос, аудио и видео имеет низкую терпимость к задержке и джиттеру, и требует приоритет над трафиком данных стандартных приложений. Поправка 802.11e определяет методы уровня 2 MAC, необходимые для выполнения требований QoS для приложений, чувствительных ко времени, в БЛВС IEEE 802.11.

Исходный стандарт 802.11 определял два метода, которыми радиокарты 802.11 могли получить контроль над полудуплексной средой. Метод по умолчанию, *Функция Распределенной Координации [Distributed Coordination Function (DCF)]*, является методом на основе борьбы, определяющим кто следующий получает право передавать в беспроводной среде.

Исходный стандарт также определял еще один метод контроля доступа к среде, с названием *Функция Координации Точкой [Point Coordination Function (PCF)]*, в которой точка доступа, если кратко, берет контроль над средой и опрашивает клиентов. Следует заметить, что метод доступа к среде PCF никогда не принимался производителями БЛВС и был удален из стандарта.



**Глава 8, "Доступ к Среде 802.11"** описывает методы DCF и PCF доступа к среде более детально.

Поправка 802.11e определяет расширенные методы доступа к среде для поддержки требований качества (QoS). *Функция Гибридной Координации [Hybrid Coordination Function (HCF)]* - это дополнительная функция координации, которая применяется в беспроводных сетях 802.11e QoS. HCF имеет два механизма доступа для обеспечения QoS. *Расширенный Распределенный Доступ к Каналу [Enhanced Distributed Channel Access (EDCA)]* это расширение DCF. Метод доступа к среде EDCA обеспечивает "приоритезацию кадров" на основе протоколов верхних уровней. Трафик таких приложений, как голос или видео, передается в режиме времени по беспроводной сети 802.11, выполняя необходимые требования по задержкам.

*Гибридная Функция Координации, Контролирующая Доступ к Каналу [Hybrid Coordination Function Controlled Channel Access (HCCA)]* является расширением PCF. HCCA дает точке доступа возможность обеспечить "приоритезацию станций". Другими словами, определенным клиентским станциям будет дан шанс передавать раньше остальных. Почти как PCF, метод доступа к среде HCCA, определенный 802.11e, никогда не принимался производителями БЛВС.

У Wi-Fi Альянса также есть сертификация с названием *Wi-Fi Мультимедиа [Wi-Fi Multimedia (WMM)]*. Сертификация WMM определяет много компонентов 802.11e, и определяет приоритезацию трафика по четырем категориям доступа с различными степенями важности. Большинство аспектов принятой QoS поправки 802.11e можно теперь найти в Статье 10 стандарта 802.11-2020.



Глава 8 охватывает 802.11e и WMM более детально.

## 802.11g-2003

Еще одна поправка, которая надела много шума на рынке Wi-Fi была опубликована как IEEE Std 802.11g-2003. Радиомодули 802.11g использовали новую технологию, с названием *Физически Расширенная Скорость [Extended Rate Physical (ERP)]*, но подразумевавшую передачу в полосе частот ISM от 2.4 ГГц до 2.4835 ГГц. Все аспекты принятой поправки 802.11g теперь можно найти в Статье 18 стандарта 802.11-2020.

Основная цель Группы по Задаче g [Task Group g (TGg)] была в улучшении Физического уровня 802.11b для того, чтобы достичь большей полосы пропускания, при этом оставаясь совместимым с MAC подуровнем 802.11. Два обязательных и два optionalных Физических уровня (PHYs) ERP были определены поправкой 802.11g.

Обязательные PHYs - это ERP-OFDM и ERP-DSSS/CCK. Для достижения более высоких скоростей передачи данных была обязательна технология PHY с названием *OFDM с Физически Расширенной Скоростью [Extended Rate Physical OFDM (ERP-OFDM)]*. С этой технологией возможно использовать скорости передачи данных в 6, 9, 12, 18, 24, 36, 48, и 54 Мбит/с,

хотя, как и с 802.11a, IEEE требовал только скорости передачи данных в 6, 12, и 24 Мбит/с. Для поддержки обратной совместимости с сетями 802.11 (только DSSS) и 802.11b, была использована технология PHY с называнием DSSS с Физически Расширенной Скоростью [*Extended Rate Physical DSSS (ERP-DSSS/CCK)*] с поддержкой скоростей передачи данных в 1, 2, 5.5, и 11 Мбит/с.

### Какая Разница между ERP-DSSS/CCK, DSSS, и HR-DSSS?

С технической точки зрения нет разницы между ERP-DSSS/CCK, DSSS, and и HR-DSSS. Ключевой момент поправки 802.11g был в поддержке обратной совместимости со старыми радиомодулями 802.11 (только DSSS) и 802.11b, и в тоже самое время достигая более высокие скорости передачи данных. Устройства 802.11g (радиомодули Статьи 18) используют ERP-OFDM для более высоких скоростей передачи данных. ERP- DSSS/CCK - это фактически та же самая технология, что и DSSS, которая используется устаревшими устройствами 802.11 (радиомодули Статьи 15) и HR-DSSS, которые используются устройствами 802.11b (радиомодули Статьи 16). Обязательная поддержка ERP-DSSS/CCK обеспечивает обратную совместимость со старыми радиомодулями 802.11 (только DSSS) и 802.11b (HR-DSSS). Технология объясняется в Главе 6.

Принятая поправка 802.11g также определяет два optionalных PHYs с названиями *ERP-PBCC* и *DSSS-OFDM*. Обе были удалены из стандарта.

### Какая разница между OFDM и ERP-OFDM?

С технической точки зрения нет разницы между OFDM и ERP-OFDM. Единственная разница в частоте передачи. OFDM указывает на устройства 802.11a (радиомодули Статьи 17), которые передают в полосах частот в 5 ГГц U-NII-1, U-NII-2, и U-NII-3. ERP-OFDM указывает на устройства 802.11g (радиомодули Статьи 18), которые передают в полосе частот 2.4 ГГц ISM. Технология объясняется детальнее в Главе 6.

Принятие поправки 802.11g запустило огромные продажи Wi-Fi устройств в небольшие предприятия и домашние офисы [small office, home office (SOHO)], и корпоративный рынок, из-за более высоких скоростей передачи данных и обратной совместимости со старым оборудованием.

Как упоминалось ранее в этой главе, разные технологии распределения спектра не могут взаимодействовать друг с другом, при этом поправка 802.11g обязана поддерживать и ERP-DSSS/CCK, и ERP-OFDM. Другими словами, технологии ERP-OFDM и ERP-DSSS/CCK могут сосуществовать, при этом они не могут говорить друг с другом. Следовательно, поправка 802.11g вызывает *защитный механизм* [*protection mechanism*], который позволяет двум технологиям сосуществовать. Цель механизма защиты ERP был в предотвращении передач от радиокарт старой 802.11b HR-DSSS или 802.11 DSSS в одно и то же время, что радиомодули 802.11g (ERP). Таблица 2.1 дает краткий обзор и сравнение 802.11, 802.11b, 802.11g, и 802.11a.

**ТАБЛИЦА 2.1** Сравнение исходных поправок 802.11

	Устаревший 802.11	802.11b	802.11g	802.11a
Частота	Полоса ISM 2.4 ГГц	Полоса ISM 2.4 ГГц	Полоса ISM 2.4 ГГц	5 ГГц полосы U-NII-1, U-NII-2 и U-NII-3
Технология расширения спектра	FHSS или DSSS	HR-DSSS	ERP: ERP-OFDM и ERP-DSSS/CCK являются обязательными	OFDM
Скорости передачи данных	1, 2 Мбит/с	DSSS: 1, 2 Мбит/с HR-DSSS: 5.5 и 11 Мбит/с	ERP-DSSS/CCK: 1, 2, 5.5, и 11 Мбит/с ERP-OFDM: 6, 12 и 24 Мбит/с являются обязательными  Также поддерживаются 9, 18, 36, 48 и 54 Мбит/с	6, 12 и 24 Мбит/с являются обязательными  Также поддерживаются 9, 18, 36, 48 и 54 Мбит/с
Обратная совместимость	Не применимо	Только 802.11 DSSS	802.11b HR-DSSS и 802.11 DSSS	Нет
Принята	1997	1999	2003	1999

## 802.11h-2003

Опубликованная как IEEE Std 802.11h-2003, эта поправка определяла механизмы для динамического выбора частоты [*dynamic frequency selection (DFS)*] и контроля мощности передачи [*transmit power control (TPC)*]. Она была изначально предложена для выполнения требований регулятора для работы в 5 ГГц полосе в Европе, и обнаружении и избегания интерференции с 5 ГГц спутниковыми и радарными системами. Эти же самые регуляторные требования были приняты FCC в Соединенных Штатах. Основное назначение DFS и TPC – это предоставить сервисы там, где передачи 5 ГГц радиомодулей 802.11 не вызовут интерференции с 5 ГГц спутниковыми и радарными передачами.

Поправка 802.11h также представила возможность для радиомодулей 802.11 передавать в новой полосе частот, называемую Расширенный U-NII-2 [*U-NII-2 Extended*], с количеством до 11 каналов, в зависимости от регуляторного домена. Поправка 802.11h, фактически, является расширением поправки 802.11a.

Технология OFDM передачи используется во всех полосах U-NII. Технологии обнаружения и избегания радара DFS и TPC определены IEEE. Однако,

организации по регулированию радиочастот в каждой стране продолжают определять радиорегулирование. В большинстве стран обнаружение радара и его избегание требуется и в полосах U-NII-2A и U-NII-2C.

DFS используется для управления спектром 5 ГГц каналов OFDM радиоустройствами. Европейский Комитет Радиосвязи [European Radiocommunications Committee (ERC)] и FCC предписывают, чтобы радиокарты, работающие в 5 ГГц полосе, применяли механизм избегания интерференции с радарными системами. DFS – это, фактически, технология обнаружения радара и избегания интерференции с радаром. Сервис DFS используется для выполнения этих регуляторных требований.

Сервис динамического выбор частоты [dynamic frequency selection (DFS)] предусматривает следующее:

- ТД позволяет клиентским станциям ассоциироваться на основе поддерживаемых каналов точки доступа. Термин ассоциироваться [*associate*] означает, что станция стала членом беспроводной сети ТД.
- ТД может замолчать на канале, чтобы проверить присутствие радара.
- ТД может протестировать канал на присутствие радара прежде, чем использовать канал.
- ТД может обнаружить радар на текущем канале и других каналах.
- ТД может прекратить работу, после обнаружения радара, чтобы избежать интерференцию.
- Когда обнаружена интерференция, ТД может выбрать другой канал для передачи и информировать об этом все ассоциированные станции.

TPC используется для регулирования уровней мощности, используемые OFDM радиокартами в 5 ГГц полосах частот. ERC предписывает, чтобы радиокарты, работающие в 5 ГГц полосе использовали TPC, чтобы соблюдать максимальную мощность передачи согласно регулирующих правил, и были способными уменьшать мощность передачи, чтобы избежать интерференции. Сервис TPC используется для выполнения требований регулятора по мощности передачи.

Сервис контроля мощности передачи [transmit power control (TPC)] обеспечивает следующее:

- Клиентские станции могут ассоциироваться с ТД на основе их мощности передачи.
- ТД и клиентские станции придерживаются разрешенных уровней максимальной мощности передачи, как разрешено регуляторами.
- ТД может указать мощность передачи любой или всех станций, которые ассоциированы с ТД.
- ТД может изменить мощность передачи на станциях на основе факторов физической радиосреды, таких как затухание на пути.

Информация, используемая и DFS, и TPC – это обмен сообщениями между клиентскими станциями и ТД внутри кадров управления. Поправка 802.11h, фактически, ввела два основных улучшения: больше частотного пространства, путем добавления Расширенной U-NII-2 [U-NII-2 Extended] полосы, и технологии избегания и обнаружения радара.

Некоторые аспекты принятой поправки 802.11h теперь можно найти в Статье 11.8 и Статье 11.9 стандарта 802.11-2020.

Стандарт DFS, наиболее часто используются для избегания радара в отличие от TPC. Тщательный анализ должен быть дан при планировании 5 ГГц БЛВС с включенными DFS каналами.



Детальное и более практическое обсуждение DFS можно найти в Главе 13 "Концепции Проектирования БЛВС". Аналогично детальное и более практическое обсуждение TPC можно найти в Главе 15 "Решение проблем БЛВС".

## 802.11i-2004

С 1997 года по 2004 год было не много определено в терминах безопасности в исходном стандарте 802.11. Три ключевых компонента любого беспроводного решения – это конфиденциальность данных (шифрование) [data privacy (encryption)], целостность данных [data integrity] (защита от модификации), и аутентификации (подтверждение личности). Семь лет единственным определенным методом шифрования в сети 802.11 было использование 64-битного статического шифрования, называемого Беспроводной Эквивалент Конфиденциальности [*Wired Equivalent Privacy (WEP)*].

Шифрование WEP долго было взламываемым и не считается приемлемым способом обеспечения конфиденциальности данных. Исходный стандарт определяет два метода аутентификации. Метод по умолчанию – аутентификация Открытой Системы [*Open System authentication*], которая, фактически, разрешает доступ всем пользователям независимо от идентификации (независимо от того, кто вы). Еще один метод называется аутентификация с Общим Ключом [*Shared Key authentication*], который «открывает ящик Пандоры» и потенциальные риски безопасности.

Поправка 802.11i, которая была принята и опубликована как IEEE Std 802.11i-2004, определяла более сильное шифрование и более лучшие методы аутентификации. Поправка 802.11i определяла надежную безопасную сеть [*robust security network (RSN)*]. Предполагаемая цель RSN была в том, чтобы спрятать данные летящие в эфире, при том в то же самое время размещая большую защиту на входе. Поправка безопасности 802.11i является без сомнения одним из наиболее важных улучшений исходного стандарта 802.11, из-за серьезности защиты беспроводной сети надлежащим образом. Основные улучшения безопасности, рассматриваемые в 802.11i это:

**Конфиденциальность Данных [Data Privacy]** Потребности в конфиденциальности решаются в 802.11i с использованием более сильного метода шифрования, называемого Протокол Режима Счетчика с Кодом Аутентификации из Шифрованных Блоков Цепочки Сообщений [*Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)*], который использует алгоритм Стандарта Улучшенного Шифрования [*Advanced Encryption Standard (AES)*]. Метод шифрования часто сокращают до CCMP/AES, AES CCMP, или просто CCMP. Поправка 802.11i также определяет optionalный метод шифрования с названием Протокол Целостности Временного Ключа [*Temporal Key Integrity Protocol (TKIP)*], который использует алгоритм потокового шифрования ARC4 и является, фактически, расширением шифрования WEP.

**Целостность Данных [Data Integrity]** Все методы шифрования БЛВС, определенные IEEE применяют механизмы целостности данных для гарантирования того, что шифрованные данные не были модифицированы. WEP использует метод целостности данных, который называется значение проверки целостности [*integrity check value (ICV)*]. TKIP использует метод, который называется проверка целостности

сообщения [*message integrity check (MIC)*]. CCMP использует намного более сильную MIC, а также другие механизмы для целостности данных. Наконец, в окончании всех кадров 802.11 находится 32-битная CRC, которая называется *последовательность проверки кадра [frame check sequence (FCS)]*, которая защищает целое тело кадра 802.11.

**Аутентификация [Authentication]** 802.11i определяет два метода аутентификации с использованием или архитектуры авторизации *IEEE 802.1X*, или заранее известных общих ключей [*preshared keys (PSKs)*]. Решение 802.1X требует использование *Протокола Расширенной Аутентификации [Extensible Authentication Protocol (EAP)]*, хотя поправка 802.11i не указывает какой метод использовать.

**Надежная Безопасная Сеть [Robust Security Network]** *Надежная безопасная сеть [robust security network (RSN)]* полностью определяет метод осуществления аутентификации, обмен сообщениями при образовании безопасных ассоциаций, и динамически генерируемые ключи шифрования для клиентских станций и точек доступа.

Все аспекты принятой поправки безопасности 802.11i теперь можно найти в Статье 12 стандарта 802.11-2020. У Wi-Fi Альянса также есть сертификация с названием *Защищенный Wi-Fi Доступ 2 [Wi-Fi Protected Access 2 (WPA2)]*, который многое повторяет из поправки безопасности IEEE 802.11i. WPA версии 1 считалась предварительной версией 802.11i, в то время как WPA версии 2 полностью совместима с 802.11i. Wi-Fi Альянс определил дальнейшие расширения безопасности Wi-Fi в обновленной сертификации WPA3.



Безопасность Wi-Fi является высшим приоритетом при развертывании БЛВС, и вот почему есть еще одна ценная сертификация, которая называется Сертифицированный Профессионал по Бесприводной Безопасности [*Certified Wireless Security Professional (CWSP)*]. Как минимум, 10 процентов экзамена CWNA включает вопросы о Wi-Fi безопасности. Следовательно, темы беспроводной безопасности—такие как 802.1X, EAP, CCMP, TKIP, WPA2, WPA3, и другие—описаны более детально в Главе 17 “802.11 Архитектура Сетевой Безопасности,” и Главе 16 “Беспроводные Атаки, Мониторинг Вторжений и Политика.”

## 802.11j-2004

Главная цель, поставленная IEEE, Рабочей группе по задаче j [Task Group j (TGj)] была в получении одобрения от Японского регулятора путем расширения 802.11 MAC и 802.11a PHY для дополнительной работы в Японии в полосах 4.9 ГГц и 5 ГГц. Не все производители БЛВС поддерживают эту полосу. Поправка 802.11j была утверждена и опубликована как IEEE Std 802.11j-2004.

В Японии радио карты 802.11 могли передавать в нижней полосе U-NII от 5.15 ГГц до 5.25 ГГц, а также в Японском лицензируемом/нелицензируемом частотном пространстве от 4.9 ГГц до 5.091 ГГц.

Радиокарты 802.11a используют технологию OFDM и требуют поддержку размера канала в 20 МГц. Когда используется 20МГц канальное пространство, то возможны скорости передачи данных в 6, 9, 12, 18, 24, 36, 48, и 54 Мбит/с с помощью технологии OFDM. В Японии также есть опция использования канального пространства OFDM в 10 МГц, что приводит к доступности ширины полосы для скорости передачи данных в 3, 4.5, 6, 9, 12, 18, 24, и 27 Мбит/с. Скорости передачи данных в 3, 6, и 12 Мбит/с

## 802.11k-2008

Цель Рабочей Группы 802.11 по Задаче k [802.11 Task Group k (TGk)] была в предоставлении средств измерения радиоресурсов [radio resource measurement (RRM)]. Поправка 802.11k-2008 вызывается для измеряемой клиентской статистической информации в форме запросов и отчетов для Физического 1ого уровня и MAC подуровня Канального [Data-Link] уровня 2. 802.11k определял механизмы, в которых данные о ресурсах клиентской станции собирались и обрабатывались точкой доступа или контроллером БЛВС [*WLAN controller*]. (Контроллеры БЛВС охвачены в Главе 11 “Архитектура БЛВС.” А пока, думайте о контроллере БЛВС, как об устройстве уровня ядра, которое управляет множеством точек доступа.) В некоторых случаях, клиент тоже может запросить информацию у точки доступа или контроллера БЛВС. Вот некоторые ключевые параметры радио ресурсов [key radio resource measurements], определенные в 802.11k:

**Контроль Мощности Передачи [Transmit Power Control]** Поправка 802.11h определила использование контроля мощности передачи [transmit power control (TPC)] для полосы 5 ГГц, чтобы уменьшить интерференцию. В 802.11k TPC также будет использоваться для других частотных полос и на территориях, управляемых другими регулирующими организациями.

**Клиентская Статистика [Client Statistics]** Информация физического уровня такая, как отношение сигнал-шум, сила сигнала, и скорости передачи данных, могут быть сообщены обратно точке доступа или контроллеру БЛВС. MAC информация такая, как передача кадров, повторы, и ошибки, также могут быть сообщены точке доступа или контроллеру БЛВС,

**Канальная Статистика [Channel Statistics]** Клиенты могут собирать информацию об уровне шума на основе радиочастотной энергии на фоне канала и сообщать эту информацию точке доступа. Информация о загрузке канала также может быть собрана и отправлена Точке Доступа. Точка доступа или контроллер БЛВС может использовать эту информацию для решений по управлению каналом.

**Отчет о Соседях [Neighbor Reports]** 802.11k дал клиентской станции способность узнавать от точки доступа или контроллера БЛВС о других точках доступа, куда клиентская станция потенциально может переключиться. Информация из отчета о соседях ТД делается доступной между устройствами БЛВС, чтобы улучшить эффективность роуминга.

С помощью проприетарных методов клиентская станция хранит у себя таблицу известных точек доступа, и принимает решения, когда переключиться на другую точку доступа. Большинство клиентских станций принимают решение о переключении на основе принятой амплитуды известных точек доступа. Другими словами, клиентская станция решает переключиться на основе своей точки зрения на радиосреду. Механизмы 802.11k предоставляют клиентской станции дополнительную информацию о существующей радиосреде.

Как определено в 802.11k, клиентская станция запросит информацию о соседних точках доступа на других каналах у точки доступа или контроллера БЛВС. Текущая ТД или контроллер БЛВС затем обработает эту информацию и создаст *отчет о соседях [neighbor report]*, уточняющий доступные точки доступа от лучшей до

худшей. Прежде чем станция переключится, она запросит отчет о соседях у текущей ТД или контроллера, а затем решит переключаться ли на одну из точек доступа из отчета о соседях. Отчеты о соседях, фактически, дают клиентским станциям больше информации о радиосреде от других существующих радиомодулей. С дополнительной информацией клиентские станции должны принять более взвешенное решение о переключении.

## 802.11n-2009

Событие, которое оказало основное потрясающее влияние на рынок Wi-Fi, было принятие поправки 802.11n-2009. С 2004 года Рабочая Группа 802.11 по Задаче n [802.11 Task Group n (TGn)] работала над улучшениями к стандарту 802.11, чтобы обеспечить более высокую пропускную способность [*greater throughput*]. Некоторые из поправок IEEE 802.11 в прошлом имели дело со скоростями передачи данных полосы пропускания в 2.4 ГГц полосе частот. Однако, конкретная цель поправки 802.11n-2009 была в увеличении пропускной способности в обеих полосах частот и в 2.4 ГГц и в 5 ГГц. Поправка 802.11n-2009 определила новый режим работы, который называется *высокая пропускная способность [high throughput (HT)]*, которая предоставляет улучшения PHY и MAC для поддержки скоростей передачи данных до 600 Мбит/с, и следовательно агрегированную пропускную способность свыше 100 Мбит/с.

Радиомодули Статьи 19 [HT Clause 19] используют технологию *много-входов, много-выходов [multiple-input, multiple-output (MIMO)]* в унисон с технологией OFDM. MIMO использует несколько принимающих и передающих антенн и, действительно, получает выгоду от эффекта многолучевого распространения [*multipath*], а не компенсирует его, чтобы уменьшить его. Выгодные последствия от использования MIMO – это увеличенная пропускная способность и даже более длинная зона действия. Радиомодули 802.11n также обратно совместимы с устаревшими радиомодулями 802.11a/b/g.



Глава 10 “Технология MIMO: HT и VHT,” обсуждает 802.11n и технологию MIMO более детально.

## 802.11p-2010

Миссия Рабочей Группы 802.11 по Задаче p [802.11 Task Group p (TGP)] была в определении улучшений к стандарту 802.11 для поддержки приложений Интеллектуальной Транспортной Системы [*Intelligent Transportation System (ITS)*]. Обмен данными между высокоскоростными транспортными средствами возможен в лицензируемой полосе ITS 5.9 ГГц. Кроме того, связь между транспортными средствами и придорожной инфраструктурой поддерживается в 5 ГГц полосах, а именно в полосе 5.850 ГГц – 5.925 ГГц в Северной Америке.

Связь может быть возможной на скорости до 200 километров в час (124 миль/час) и на расстоянии 1000 метров (3281 футов). Также нужны очень малые задержки, так как некоторые приложения должны гарантировать доставку данных в пределах от 4 до 50 миллисекунд.

802.11p также называется как *Беспроводной Доступ в Транспортных Средах [Wireless Access in Vehicular Environments (WAVE)]* и является возможной основой для проекта Министерства Транспорта США, который называется Выделенная Связь на Коротких Дистанциях [*Dedicated Short Range Communications (DSRC)*]. Проект DSRC предполагает общенациональную транспортную и придорожную сеть связи, использующую такие приложения, как сервисы транспортной безопасности, предупреждения об автомобильных «пробках», пункты взимания платы, предотвращение столкновения транспорта, и адаптивное управление светофорами. В Европе,

Интеллектуальная Транспортная Система ETSI основана на технологии IEEE 802.11 и 802.11р. Этот стандарт создан для предоставления связи транспортное средство-транспортное средство и транспортное средство-инфраструктура. 802.11р также будет применим к морской и железнодорожной связи.

Пожалуйста, учтите, что практическое внедрение технологии 802.11р еще не состоялось. В Главе 6 вы узнаете, что другая радиотехнология, новая сотовая LTE технология, которая называется сотовая технология транспортное средство-ко-всеми [*cellular vehicle-to-everything (C-V2X)*], более вероятно будет использоваться.

## **802.11r-2008**

Поправка 802.11r-2008, которая называется как поправка *быстрого перехода базового состава сервиса* [*fast basic service set transition (FT)*]. Технология более часто называется как *быстрый безопасный роуминг* [*fast-secure roaming*], потому что он определяет быструю передачу обслуживания [*handoffs*], когда происходит переключение (роуминг) между зонами покрытия в БЛВС, использующие сильную безопасность, определенную надежной безопасной сетью [*robust secure network (RSN)*]. Знайте, что существует несколько типов быстрого безопасного роуминга, которые применяются разными производителями. Они включают ССКМ, РКС, ОКС, и быстрое возобновление сеанса [*fast session resumption*]. Некоторые производители поддерживают 802.11r, в то время как другие нет.

802.11r был предложен в первую очередь из-за временных ограничений приложений таких, как VoWiFi. Среднее время задержки составляет сотни миллисекунд, когда клиентская станция переключается с одной точки доступа на другую точку доступа.

Роуминг может быть особенно проблемным при использовании решений безопасности WPA2-Enterprise или WPA3-Enterprise, который требуют использование сервера RADIUS для аутентификации 802.1X/EAP и часто занимает 700 миллисекунд или больше для клиентской аутентификации. VoWiFi требует переключение в 100 миллисекунд или меньше, чтобы избежать деградации качества звонка или, что еще хуже, потери соединения.

В 802.11r клиентская станция способна установить поток с поддержкой качества (QoS) и установить безопасную ассоциацию с новой точкой доступа эффективным способом, который позволяет свободно пройти аутентификации 802.1X/ EAP при переключении на новую точку доступа. Клиентская станция способна достичь выполнения этих задачи или по кабелю до исходной точки доступа или через эфир. Фактически, клиентская станция завершит процесс переключения и перейдет на новую точку доступа.

Тактически корпоративная установка этой технологии чрезвычайно важна для обеспечения более безопасной связи для VoWiFi. Подробности этой технологии в значительной степени проверяются на экзамене CWSP.

## **802.11s-2011**

Поправка 802.11s-2011 была принята в Июле 2011 года. Точки доступа 802.11 обычно действуют как портальные устройства в *систему распределения* [*distribution system (DS)*], которая обычно является проводной 802.3 Ethernet средой. Стандарт 802.11-2020, однако, не обязывает, чтобы система распределения использовала проводную среду. Точки доступа могут, следовательно, действовать как портальные устройства в *беспроводную систему распределения* [*wireless distribution system (WDS)*]. Поправка 802.11s предлагает использование протокола для адаптивных, автоматически настраивающихся систем, которые

поддерживают широковещательный [broadcast], многоадресный [multicast], и однодиаправленный [unicast] трафик через много скачковую [multi-hop] взаимосвязываемую [mesh] WDS.

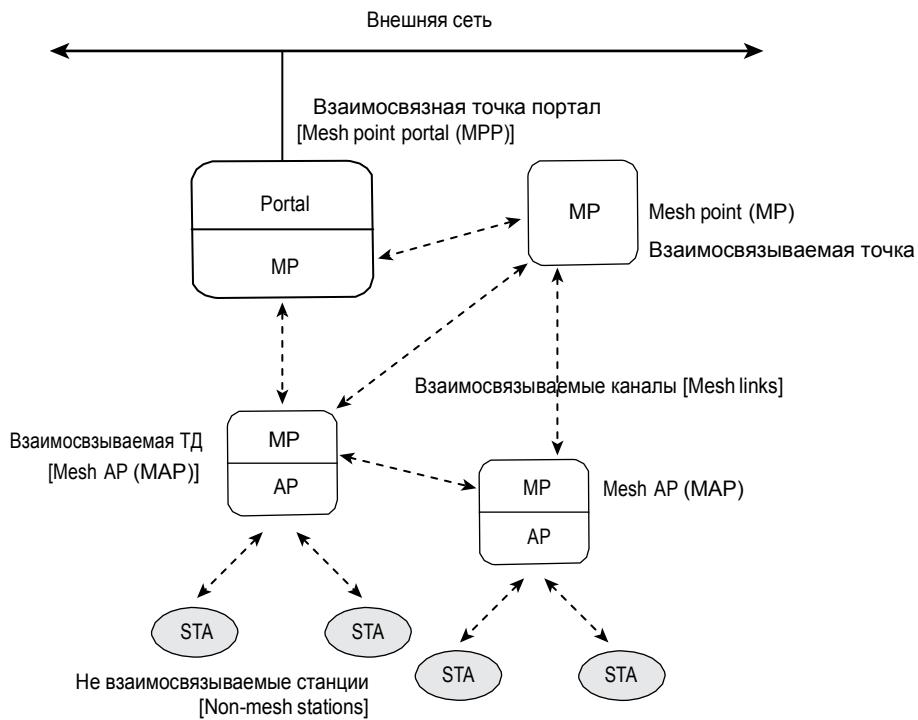
Рабочая Группа по Задаче s [802.11 Task Group s (TGs)] выразила стремление по стандартизации взаимосвязываемой сетевой работы [*mesh networking*] с помощью уровней MAC/PHY IEEE 802.11. Поправка 802.11s определила использование взаимосвязываемых точек [mesh points (MPs)], которые являются станциями с поддержкой 802.11 QoS, который поддерживают взаимосвязываемые [mesh] сервисы.

Взаимосвязываемая точка [mesh point] способна использовать обязательный взаимосвязываемый [mesh] протокол маршрутизации, который называется *Гибридный Беспроводной Взаимосвязываемый Протокол* [*Hybrid Wireless Mesh Protocol (HWMP)*], который использует метрики выбора пути по умолчанию. Как показано на Рисунке 2.2, взаимосвязываемая точка доступа [mesh access point (MAP)] - это устройство, которое обеспечивает и функциональность взаимосвязываемости [mesh] и функциональность ТД одновременно. *Взаимосвязанная точка портал* [mesh point portal (MPP)] - это устройство, которое действует как шлюз к одной или более внешних сетей, таких как 802.3 проводная опорная сеть. Несмотря на принятие 802.11s, большинство производителей БЛВС используют проприетарные взаимосвязываемые [mesh] протоколы маршрутизации и метрики, которые частично базируются на HWMP.



Дальнейшее обсуждение системы распределения [distribution systems (DSs)] и беспроводной системы распределения [wireless distribution systems (WDSs)] можно найти в Главе 7 "Топологии Беспроводных ЛВС." Вы узнаете больше о взаимосвязываемой сетевой работе 802.11 [802.11 mesh networking] в Главе 11.

**РИСУНОК 2.2** Взаимосвязываемые [mesh] точки, взаимосвязываемы [mesh] ТД, и взаимосвязываемый [mesh] портал.



## 802.11u-2011

Первичная цель Рабочей Группы 802.11 по Задаче u [802.11 Task Group u (TGu)] была в решении вопросов межсетевого взаимодействия между сетями доступа IEEE 802.11 и любыми внешними сетями, к которым они подключены. Нужен общий подход для интеграции сетей доступа 802.11 с внешними сетями в универсальном и стандартизированном виде. 802.11u также часто называется как *Беспроводное Межсетевое Взаимодействие с Внешними Сетями* [Wireless Interworking with External Networks (WIEN)].

Поправка 802.11u-2011, принятая в Феврале 2011 года, определила функции и процедуры для помощи STA при обнаружении и выборе сети, передачу информации из внешних сетей с помощью распределения по классам качества сервиса [QoS], и общие механизмы для поддержки экстренных служб.

Поправка 802.11u-2011 является основой для спецификации Wi-Fi Альянса Хотспот 2.0 и ее сертификации Паспойнт [Passpoint]. Этот стандарт и сертификация спроектированы для обеспечения незаметного переключения беспроводных устройств между вашей Wi-Fi сетью и другими партнерскими сетями, аналогично тому, как сети сотовой телефонии обеспечивают роуминг. Паспойнт [Passpoint] и Хотспот 2.0 [Hotspot 2.0] обсуждаются более детально в Главе 18 "Приноси Собственное Устройство (BYOD) и Гостевой Доступ".

## 802.11v-2011

Поправка 802.11v-2011 была принята в Феврале 2011 года. Если 802.11k определяет методы получения информации от клиентских станций, 802.11v обеспечивает обмен информацией, которая может потенциально упростить настройку клиентской станции по беспроводной связи из центральной точки управления. 802.11v-2011 определяет *беспроводное сетевое управление* [*wireless network management (WNM)*], которое дает станциям 802.11 возможность обмена информации в целях улучшения общей производительности беспроводной сети. Точки доступа и клиентские станции используют протоколы WNM для обмена рабочими данными так, чтобы каждая станция знала о состоянии сети, позволяя станциям быть более осведомленными о топологии и состоянии сети.

В дополнение к предоставлению информации о состоянии сети, протоколы WNM определяют механизмы, в которых устройства БЛВС могут обмениваться информацией о местоположении, обеспечивать поддержку функционала нескольких BSSID, и предлагают новый режим WNM-Sleep, в котором клиентская станция может уходить в спящий режим на более длительные периоды времени без получения кадров от ТД.

Некоторые из механизмов 802.11v определены Wi-Fi Альянсом как optionalные механизмы в сертификации Голосовой Связи на Предприятии [Voice-Enterprise].

## 802.11w-2009

Распространенный тип атаки на БЛВС 802.11 – это атака отказа-в обслуживании [*denial-of-service (DoS)*]. Существует множество DoS атак, которые могут быть запущены против беспроводной сети; однако, самая распространенная DoS атака осуществляется на 2ом уровне с помощью кадров управления 802.11. Это просто, когда атакующий редактирует кадры деаутентификации [*deauthentication*] или диассоциации [*disassociation*], и затем повторно передает кадры в эфир, фактически выключая беспроводную сеть.

Цель Рабочей Группы IEEE по Задаче w [IEEE Task Group w (TGw)] была в предоставлении способа доставки кадров управления безопасным способом, предотвращая, таким образом, подделку кадров управления. Поправка 802.11w-2009 предоставила защиту однонаправленных [*unicast*], широковещательных [*broadcast*], и многоадресных [*multicast*] кадров управления.

Эти кадры 802.11w называются как *надежные кадры управления* [*robust management frames*]. Надежные кадры управления могут быть защищены сервисом защиты кадров управления, и включают кадры диассоциации, деаутентификации, и надежные кадры действия. Кадры действия используются для запроса станции выполнить действие от имени другой станции, и не все кадры действия надежны.

Когда однонаправленные [*unicast*] кадры управления защищены, защита кадров достигается с помощью ССМР. Широковещательные [*Broadcast*] и многоадресные [*multicast*] кадры защищены с помощью *Широковещательного/Многоадресного Протокола Целостности* [*Broadcast/Multicast Integrity Protocol (BIP)*]. BIP обеспечивает целостность данных и воспроизводит защиту с помощью AES-128 в режиме Кода Сообщения Аутентификации на Основе Шифра [Cipher-Based Message Authentication Code (CMAC)]. Стоит отметить, что поправка 802.11w не кладет конец всем DoS атакам 2ого уровня. Однако, многие механизмы *защиты кадров управления* [*management frame protection (MFP)*], определенные в 802.11w теперь являются обязательными требованиями для сертификации безопасности WPA3 от Wi-Fi Альянса.



Вы найдете обсуждение о DoS атаках уровня 1 и уровня 2 в Главе 16.

## 802.11y-2008

Хотя устройства 802.11 в основном работают в нелицензируемых частотах, они могут также работать на частотах, которые лицензируются национальными регулирующими организациями.

Цель Рабочей Группы IEEE по Задаче y [IEEE Task Group y (T Gy)] была в стандартизации механизма, требуемого для разрешения высокой мощности, совместной работы 802.11 с другими не-802.11 устройствами в лицензируемой полосе 3650 МГц–3700 МГц в Соединенных Штатах. Стоит отметить, что механизмы, определенные поправкой 802.11y-2008 могут быть использованы в других странах и других лицензируемых частотах.

Лицензируемая полоса от 3650 МГц до 3700 МГц требует механизмов протокола на основе содержания [content-based protocol (CBP)] для предотвращения интерференции между устройствами. Метод борьбы за среду CSMA/CA (который используется радиомодулями Wi-Fi), обычно подходит по эти требования. Однако, когда метода CSMA/CA не достаточно, поправка 802.11y-2008 определяет процедуры динамического включения STA [*dynamic STA enablement (DSE)*]. Радиомодули 802.11 широко вещают [*broadcast*] свое реальное местоположение в качестве уникального идентификатора, для того, чтобы помочь решить вопрос с интерференцией с не-802.11 радиомодулями на той же частоте.

## 802.11z-2010

Целью Рабочей Группы IEEE по Задаче z [IEEE Task Group z (TGz)] было создание и стандартизация механизма установки прямого канала связи [*direct link setup (DLS)*], чтобы разрешить работу с точками доступа без DLS возможности. В большинстве сред БЛВС весь обмен кадров между клиентскими станциями, которые ассоциированы с одной и той же точкой доступа, должен проходить через эту точку доступа. DLS позволяет клиентским станциям проходить мимо точки доступа и поддерживать связь прямым обменом кадров. Некоторые ранние поправки определяли связь DLS. Поправка 802.11z-2010 определила улучшения к DLS связи. Стоит отметить, что связь DLS еще не использовалась производителями корпоративных БЛВС.

## 802.11aa-2012

Поправка 802.11aa специфицирует улучшения QoS к Контролю Доступа к Среде 802.11 [802.11 Media Access Control (MAC)] для надежной передачи аудио и видео потоков как для потребительских, таки для корпоративных приложений. 802.11aa обеспечивает улучшенное управление, увеличенную надежность канала связи, и увеличенную производительность приложений. Поправка определяет *Вещание на Группу с Повторами* [*Groupcast with Retries (GCR)*], гибкий сервис для улучшения доставки кадров адресованных группе. GCR может быть предоставлен инфраструктурой BSS ТД своим ассоциированным STA или во взаимосвязываемой [mesh] BSS взаимосвязываемым [mesh] STA и ее одноуровневым [peer] взаимосвязываемым [mesh] STA.

## 802.11ac-2013

Поправка 802.11ac-2013 определяет расширение очень высокой пропускной

способности [very high throughput (VHT)] ниже 6 ГГц. Технология используется только в 5 ГГц полосах частот, где уже работают радиомодули 802.11a/n. 802.11ac использует преимущества большего спектрального пространства, чем могут предоставить 5 ГГц полосы U-NII.

Полоса ISM 2.4 ГГц не может предоставить необходимое пространство частот, чтобы быть способной использовать все преимущества технологии 802.11ac. Чтобы воспользоваться всеми преимуществами 802.11ac, еще больший спектр был бы предпочтительнее в 5 ГГц. Поправка 802.11ac определяет максимальную скорость передачи данных в 6933.3 Мбит/с. 802.11ac предоставляет гигабитные скорости с помощью следующих четырех улучшений:

**Более Широкие Каналы** 802.11n представила возможность 40 МГц каналов, которые фактически удваивали скорости передачи данных. 802.11ac поддерживает ширины каналов 20 МГц, 40 МГц, 80 МГц, и 160 МГц. Это основная причина, по которой корпоративные радиомодули 802.11ac не смогут работать в полосе 2.4 ГГц ISM.

**Новая Модуляция** 802.11ac предоставляет возможность использовать модуляцию 256-QAM, которая может обеспечить, по крайней мере, 30 процентов увеличения по скорости по сравнению с предыдущими методами модуляции. Модуляция 256-QAM требует очень высокого отношения сигнал-шум (SNR), чтобы эффективно работать.

**Больше Пространственных Потоков** В соответствии со стандартом, радиомодули 802.11ac могут быть изготовлены так, чтобы передавать и принимать до восьми пространственных потоков. В действительности, первая пара поколений чипсетов 802.11ac поддерживает только до четырех пространственных потоков.

**Улучшенное MIMO и Формирование луча [Beamforming]** В то время как 802.11n определила использование однопользовательских радиомодулей MIMO, очень высокая пропускная способность [very high throughput (VHT)] представила использование технологии многопользовательского MIMO [*multi-user MIMO (MU-MIMO)*]. Точка доступа с поддержкой MU-MIMO может передавать сигнал нескольким клиентским станциям на том же самом канале одновременно, если клиентские станции поддерживают MU-MIMO и находятся физически в разных местах. 802.11ac может использовать явное формирование луча [*explicit beamforming*].



Технология 802.11ac была представлена двумя поколениями чипсетов, часто называемых волнами [*waves*]. Первая волна [*wave*] чипсетов 802.11ac использовала модуляцию 256-QAM и каналы до 80 МГц. В основном аппаратная часть ТД использует радиомодули 3x3:3. Вторая волна [*wave*] чипсетов 802.11ac обычно может использовать MU-MIMO и каналы до 160 МГц. Нужно понимать, что термин волна [*wave*] - это чисто маркетинговый термин при обсуждении поколений радиомодулей 802.11ac. Аппаратная часть ТД также поддерживает радиомодули 4x4:4. Глава 10 в значительной степени посвящена 802.11ac-2013 и нынешних технологиях.

## 802.11ad-2012

Поправка 802.11ad определяет улучшения производительности, используя более высокую нелицензируемую полосу частот 60 ГГц и способ передачи, который называется *направленный мультигигабит* [*directional multigigabit (DMG)*]. Более

высокий диапазон частот достаточно большой, чтобы поддержать скорости передачи данных до 7 Гбит/с. Обратная сторона в том, что у 60 ГГц значительно меньшая дальность действия, чем у 5 ГГц сигнала, и ограничена до связи в прямой видимости, так как высокочастотному сигналу сложно проникать через стены. Сертификационная программа СЕРТИФИЦИРОВАННЫЙ Wi-Fi WiGig [Wi-Fi CERTIFIED WiGig] основан на технологии, изначально определенной в поправке 802.11ad для направленных мультигигабитных [directional multigigabit (DMG)] радиомодулей, которые передают в полосе частот 60 ГГц.

Wi-Fi технология 60 ГГц имеет потенциал для использования для беспроводных док станций, беспроводных дисплеев, проводного эквивалента передачи данных, и потокового несжатого видео. 60 ГГц Wi-Fi технология также может быть использована для каналов связи точка-точка на короткие расстояния до 1/4 мили (400 м), однако дождь может помешать связи, поэтому может понадобится запасной 5 ГГц канал связи (некоторые ТД содержат оба радиомодуля в корпусе одной и той же ТД по этой причине). Чтобы обеспечить незаметный переход при переключении между 60 ГГц полосой частот и старыми полосами 2.4ГГц и 5 ГГц, к спецификации была добавлена характеристика "быстрая передача сеанса" [“fast session transfer”].

Технология DMG также требует принятия новых механизмов шифрования. Были сомнения в том, что текущий метод шифрования CCMP сможет надлежащим образом обработать предполагаемые высокие скорости передачи данных. CCMP использует два соединенных вместе криптографических режима AES для обработки 128-битных блоков данных. 128-битные блоки данных должны также быть обработаны "по порядку" от первого режима AES криптографии ко второму режиму.

Поправка 802.11ad специфицирует использование *Протокол Режима Счетчика/Галуа* [Galois/Counter Mode Protocol (GCMP)], который также использует криптографию AES. Однако, вычисления GCMP могут выполняться параллельно и менее вычислительно интенсивны, чем криптографические операции CCMP.

### Что Случилось с Беспроводным Гигабитным Альянсом?

Беспроводной Гигабитный Альянс [Wireless Gigabit Alliance (WiGig)] был образован для продвижения беспроводной связи в потребительской электронике, ручных устройствах, и ПК, используя уже доступный нелицензируемый спектр 60 ГГц. Зего Января 2013 года было анонсировано, что деятельность WiGig Альянса будет объединена с Wi-Fi Альянсом. С тех пор Wi-Fi Альянс активно работает и под брендом WiGig и испытаниями при сертификации продуктов.

## 802.11ae-2012

Поправка 802.11ae специфицирует улучшения к управлению качеством [QoS]. Можно включить сервис качества обслуживания кадров управления [quality-of-service management frame (QMF)], позволяя некоторым кадрам управления быть переданными с помощью категории доступа QoS, которая отличается от категории доступа, присвоенной голосовому трафику. Это может улучшить качество сервиса потоков другого трафика.

## 802.11af-2014

Поправка 802.11af разрешает использование беспроводной связи в *Телевизионном белом пространстве частот* [TV white space (TVWS)] между 54 МГц и 790 МГц. Эта технология иногда называется как *White-Fi* или *Super Wi-Fi*, но мы рекомендуем, чтобы вы

остерегались использовать эти термины, так как эта технология не связана с Wi-Fi Альянсом, который является держателем торговой марки термина Wi-Fi.

В разных регионах или на разных ТВ рынках используются не все из доступных ТВ каналов лицензированными станциями. TVWS - это диапазон ТВ частот, которые не используются лицензированными станциями на определенной территории. Радиомодули основанные на 802.11af должны будут проверять, что частоты доступны, и убеждаться, что они не создадут интерференции. Чтобы этого достичь, ТД 802.11af сначала нужно определить свое местоположение, вероятнее всего с использованием технологии GPS. Затем радиоустройству нужно связаться с географической базой данных, чтобы определить доступные каналы для данного времени и места.

Физический уровень основан на технологии OFDM, используемой в 802.11ac, но с использованием меньших по ширине каналов, чем 802.11ac, и с максимум четырьмя пространственными потоками. Этот новый Физический уровень (PHY) называется *телевизионная очень высокая пропускная способность [television very high throughput (TVHT)]*, и спроектирован для поддержки узких ТВ каналов, которые сделаны доступными телевизионным белым пространством частот [TVWS].

Используемые частоты с малой шириной полосы означают меньшие скорости передачи данных по сравнению с технологией 802.11a/b/g/n/ac/ax. Максимальная скорость передачи - это 26.7 Мбит/с или 35.6 Мбит/с, в зависимости от ширины канала, который определяется регуляторным доменом. Ширина канала между 6 МГц и 8 МГц, и до четырех каналов может быть объединено вместе. Радиомодули 802.11af могут поддерживать до четырех пространственных потоков. Используя четыре канала и четыре пространственных потока, 802.11af имеет максимальную скорость передачи данных около 426 Мбит/с или 568 Мбит/с, в зависимости от регуляторного домена. Хотя низкие частоты TVWS означают низкие скорости передачи данных, низкие частоты обеспечивают передачу на более далекие расстояния, вместе с более лучшим проникновением через такие препятствия, как листва и здания. Это большее расстояние может дать в результате покрытие, которое является более проникающим, обеспечивающим смежный роуминг вне помещений в офисных парках, кампусах, или публичных сетей сообществ. Еще одно предполагаемое применение - это предоставление широкополосного сервиса доступа в Интернет в сельской местности.

Важно отметить, что стандарт IEEE 802.22-2011 также специфицирует беспроводную связь в телевизионном белом пространстве частот. Это может стать причиной проблем существования в будущем между этими конкурирующими технологиями. Также, существование нескольких технологий в одном и том же частотном пространстве может разделить разработку и принятие продуктов.

## 802.11ah-2016

Поправка 802.11ah определяет использование Wi-Fi в частотах ниже 1 ГГц.

Сертификация *Wi-Fi HaLow* от Wi-Fi Альянса основана на механизмах, определенных в поправке IEEE 802.11ah. Низкие частоты означают низкие скорости передачи данных, но на далекие расстояния. Вероятное применение 802.11ah будет в сетях сенсоров вместе с транзитными каналами для сенсорных сетей, и с Wi-Fi с увеличенной зоной обслуживания таких, как умные дома, автомобили, здравоохранение, промышленность, розничные магазины, и сельское хозяйство. Эта межсетевая работа устройств называется как Интернет Вещей [*Internet of Things (IoT)*] или межмашинная [*machine-to-machine (M2M)*] связь.

Доступные частоты варьируются между странами. Например, нелицензируемые ISM частоты 902–928 МГц доступны в Соединенных Штатах, в то время как частоты 863–868 МГц вероятно будут доступны в Европе, а частоты 755–787 МГц вероятно будут доступны в Китае.

## 802.11ai-2016

Цель поправки 802.11ai в обеспечении *быстрой начальной установки канала связи* [*fast initial link setup (FILS)*]. Он создан чтобы решить проблемы, которые присутствуют в средах с высокой плотностью, где большое количество мобильных пользователей непрерывно присоединяются и отсоединяются от расширенного состава сервиса [ESS]. Поправка создана для улучшения подключения пользователя в средах с высокой плотностью таких, как аэропорты, спортивные стадионы, арены, и торговые центры. FILS особенно важен для гарантии того, что каналы ассоциаций надежной защищенной сети [*robust security network association (RSNA)*] не деградируют при клиентском роуминге.

## 802.11aj-2018

Поправка 802.11aj предоставляет модификацию уровней PHY и MAC поправки IEEE 802.11ad-2012, чтобы обеспечить работу в полосах частот Китайских Миллимитровых Волн [Chinese Millimeter Wave (CMMW)]. Полосы частот CMMW - это 59–64 ГГц. Поправка также предоставляет модификацию уровней PHY и MAC поправки IEEE 802.11ad-2012, чтобы обеспечить поддержку работы в Китайской полосе частот 45 ГГц.

## 802.11ak-2018

Поправка 802.11ak также называется как *Основной Канал Связи* [*General Link (GLK)*]. Поправка предоставляет улучшения к каналам связи 802.11 для использования в сетях типа мост [*bridged networks*]. Эти сети типа мост будут оцениваться как потенциальная поддержка домашних развлекательных систем, промышленных контрольных устройств, и других продуктов, у которых есть и беспроводные 802.11 и проводные 802.3 возможности. GLK нацелен на упрощение использования 802.11 между точками доступа и беспроводными станциями, позволяя станциям предоставлять сервисы мостов.

## 802.11aq-2018

Сервис пре-ассоциации 802.11aq [*802.11aq pre-association service*] позволяет предоставить информацию о сетевых сервисах до ассоциации станции с сетью 802.11. Цель в предоставлении оповещения станции о сервисах до того как станция реально ассоциируется с сетью.

# IEEE 802.11, Черновые Поправки

Что подготовило будущее для нас в части беспроводных сетей 802.11? Черновые поправки - это подзорная труба в улучшения и возможности, которые могут стать доступными в ближайшем будущем для устройств беспроводных сетей 802.11. Еще большая эффективность сетевой пропускной способности ждет нас на беспроводном горизонте.

Важно помнить, что черновые поправки являются предложениями, которые еще не приняты. Хотя некоторые производители уже могут продавать продукты, которые имеют некоторые возможности, описанные в следующих разделах, эти характеристики часто считаются проприетарными. Даже если производитель может выводить на рынок эти предстоящие к принятию возможности, это не гарантирует, что их продукты будут работать с будущими продуктами, которые сертифицированы как совместимые с грядущей принятой поправкой. Держа это в уме, вспоминаем, что IEEE не сертифицирует Wi-Fi технологии, вместо этого, Wi-Fi Альянс сертифицирует функциональность и совместимость радиомодулей 802.11. Например, несмотря на тот факт, что 802.11ax является все еще черновой поправкой IEEE, Wi-Fi Альянс сертифицирует технологию 802.11ax с августа 2019 года по сертификации Wi-Fi 6. Поэтому, иногда технологии являются рабочими и сертифицированными на рынке несмотря на то, что еще не полностью приняты IEEE.



Экзамен CWNA (CWNA-108) на текущий момент охватывает все технологии, определенные в стандарте 802.11-2020, а также все поправки принятые с 2020 года. За исключением 802.11ax, вы не будете проверяться на знание черновых поправок. И даже при этом, мы полагаем, что это важно для Вас быть в курсе технологий, которые планируются и разрабатываются, так как они вероятнее всего могут изменить беспроводные сети 802.11 в будущем.

Оставшиеся страницы в этой главе дают беглый взгляд в будущее более продвинутых и изысканных Wi-Fi продуктов, которые могут поднять эту технологию на еще большие высоты. Еще раз, пожалуйста, помните, что эти поправки IEEE все еще черновые документы, и они вероятнее всего будут другими в финальных, принятых поправках.

## 802.11ax (Высокая Эффективность)

Черновая поправка 802.11ax, которая называется поправка БЛВС *высокой эффективности* [*high efficiency (HE)*], ожидается, что будет следующим большим улучшением PHY в стандарте 802.11. 802.11ax будет работать в полосах частот 2.4 ГГц, 5 ГГц и 6 ГГц. В дополнение к увеличению клиентской пропускной способности, она проектируется для обеспечения поддержки большего количества пользователей и сред высокой плотности. Глава 19 “802.11ax: Высокая Эффективность High Efficiency (HE),” – посвящена 802.11ax. Хотя ранние поправки определяли методы для достижения более высоких скоростей передачи данных, 802.11ax использует улучшения уровня PHY и MAC для более лучшего управления трафиком существующей среды БЛВС. Ключевая компонента 802.11ax это технология множественного доступа с ортогональным частотным разделением [*orthogonal frequency-division multiple access (OFDMA)*]. OFDMA является многопользовательской версией популярной цифровой схемы модуляции – ортогональное мультиплексирование с частотным разделением [*orthogonal frequency-division multiplexing (OFDM)*]. Множественный доступ достигается в OFDMA путем назначения поднаборов несущих отдельным клиентам. Это позволяет одновременно осуществлять низкоскоростную передачу данных к/от нескольких пользователей.



В то время, когда это писалось поправка 802.11ax еще не была принята. Однако, технология на рынке уже свыше двух лет и подтверждается Wi-Fi Альянсом в сертификации Wi-Fi 6. 802.11ax является большим сдвигом парадигмы от предыдущих поправок, потому что сфокусирована на эффективности, а не на более высоких скоростях передачи данных. Очень подробную информацию о том, как радиомодули Wi-Fi 6 и 802.11ax работают можно найти в Главе 19.

## 802.11ay (Следующее Поколение 60 ГГц)

Черновая поправка 802.11ay будет определять модификации обоих уровней PHY и MAC 802.11, и ожидается, что будет способна поддерживать максимальную пропускную способность, по крайней мере, 20 Гбит/с при этом поддерживая или улучшая энергетическую эффективность станции. 802.11ay будет работать в нелицензируемых полосах выше 45 ГГц, и будет обеспечивать обратную совместимость с 802.11ad. Ожидается, что 802.11ay будет основой для следующего поколения БЛВС в 60 ГГц.

## 802.11az (Позиционирование Следующего Поколения)

Одна из целей 802.11az – это улучшение отслеживания физического местоположения и определения местоположения устройств 802.11. Она будет определять модификацию обоих уровней и PHY, и MAC, которые позволят делать абсолютную и относительную оценку местоположения с высокой точностью. Лучшая точность может быть использована с приложениями умных зданий и отслеживающих IoT устройств, обеспечивая следующее поколение определения местоположения с помощью БЛВС. Еще одна цель этой поправки в увеличении энергоэффективности сети, включая характеристики безопасности.

## 802.11ba (Пробуждаемый Радиомодуль)

Ожидается, что эта поправка определит энергоэффективный режим получения данных, называемый *пробуждаемый радиомодуль* [*wake-up radio(WUR)*]. Цель в увеличении срока жизни аккумуляторной батареи таких устройств, как IoT устройства, без увеличения сетевой задержки или уменьшения производительности.

## 802.11bb (Световая Связь)

Ожидается, что эта поправка определит спецификацию (параметры) связи на основе света. Поправка определит несколько новых спецификаций физического уровня [PHY] и определит новую спецификацию канального уровня [MAC]. Ожидается, что связь будет работать в полосе 380-5000 нанометров (нм). Цель - это минимальная пропускная способность одного канала от 10 Мб/с до 5 Гб/с. Эта технология называется как *Li-Fi*.

## 802.11bc (Расширенный Широковещательный Сервис)

Ожидается, что эта поправка, которая называется как Расширенный Широковещательный Сервис [Enhanced Broadcast Service (BCS)], модифицирует спецификацию второго уровня

[MAC], чтобы включить расширенную передачу и прием широковещательных [broadcast] данных в среде инфраструктуры BSS и в средах, где нет ассоциации между предатчиком(-ами) и приемником(-ами). Это расширит зону действия широковещательных данных БЛВС.

## 802.11bd (Улучшения для V2X Следующего Поколения)

Цель этой поправки в развитии технологий радио доступа [radio access technologies (RAT)], которые обеспечивают надежную с низкой задержкой связь транспортное средство-со -всеми [vehicle-to-everything (V2X)] с помощью выделенной связи на короткой дистанции [dedicated short-range communications (DSRCs)]. DSRC создана для работы в первую очередь в полосе 5.9 ГГц и опирается на 802.11p для своих уровней PHY и MAC.

## 802.11be (Чрезвычайно Высокая Пропускная Способность)

Поправка *чрезвычайно высокой пропускной способности* [*extremely high throughput (EHT)*] была разработана для обеспечения следующего большого увеличения в скорости и производительности, предоставляя скорости передачи данных в 40 Гбит/с. Ожидается, что 802.11be масштабирует технологии 802.11ax путем удвоения ширины полосы пропускания [bandwidth] и увеличения пространственных потоков; однако, также ожидается, что будет представлено много революционных изменений, которые сами предоставляют основу для дальнейшей эволюции БЛВС. Ожидается, что эта технология будет доступна через три-пять лет и может в будущем называться как технология Wi-Fi 7. Будущее еще предстоит увидеть.

# Нерабочие Поправки

Следующие две поправки никогда не были приняты и считаются канувшими в лету. Однако, суть темы (тестирование производительности и роуминг) двух поправок важен, и следовательно мы будем обсуждать их в этой книге.

## 802.11F

Рабочая Группа IEEE по Задаче F [IEEE Task Group F (TGF)] опубликовала IEEE Std 802.11F-2003 как рекомендованную практику в 2003 году. Поправка никогда не была принята и была отозвана в феврале 2006 года.



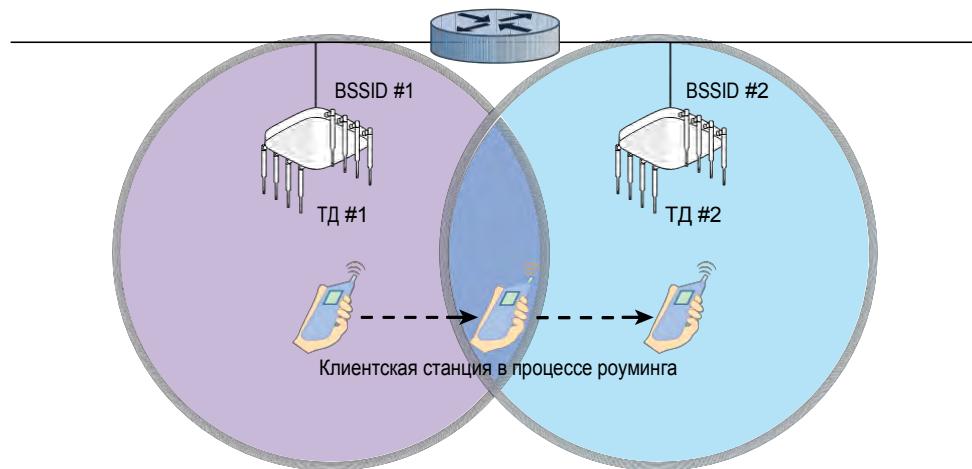
Использование заглавной буквы в обозначении рабочей группы IEEE по задаче, как в Рабочей Группе IEEE по Задаче F [IEEE Task Group F], означает, что эта поправка (F) считается рекомендуемой практикой, а не частью стандарта.

Изначально опубликованный стандарт 802.11 обязывал производителей ТД поддерживать роуминг [*roaming*]. Механизм, который нужен, чтобы позволить клиентским станциям, которые уже на связи через одну ТД, иметь возможность выпрыгнуть из зоны покрытия исходной ТД и продолжить поддерживать связь через новую ТД. Незаметный (бесшовный) роуминг [*Seamless roaming*] обеспечивает мобильность, которая является

### Будет ли Работать Бесшовный Роуминг, Если Я Смешаю и Расставлю Точки Доступа Разных производителей?

Ответ в реальном мире - нет. 802.11F был предназначен для решения совместимости роуминга между автономными точками доступа [*autonomous access points*] от разных производителей. Поправка 802.11F была изначально только рекомендованной практикой, и была, фактически, полностью отозвана IEEE. Производители БЛВС хотели, чтобы заказчики покупали только те бренды ТД, которые продаёт производитель, а не ТД конкурентных брендов."Рекомендованная практика" этой книги - это не смешивать точки доступа разных производителей в одном и том же проводном сегменте сети. Роуминг обсуждается более подробно в Главах 7, 9 и 15.

**РИСУНОК 2.3** Ровное переключение или незаметный роуминг



Хотя стандарт 802.11 требует поддержку роуминга, он не предписывает как роуминг должен в действительности осуществляться. IEEE изначально предполагал, что производители должны иметь гибкость в применении проприетарных механизмов роуминга ТД-ТД. Поправка 802.11F была попыткой стандартизовать то, как механизмы роуминга работают за кулисами в среде системы распределения, которая обычно является сетью 802.3 Ethernet, использующая сетевые протоколы TCP/IP. 802.11F решала вопрос "совместимости производителей" для роуминга ТД-ТД. Финальным результатом была рекоммендуемая практика по использованию *Протокола Между Точками Доступа* [*Inter-Access Point Protocol (IAPP)*]. IAPP использовал оповещения и процесс передачи обслуживания [handover], который приводил к тому, что ТД информировала другие ТД о переключающихся клиентах, а также о доставке забуферизованных пакетов. Так как поправка 802.11F никогда не была принята, использование IAPP в основном не существенно.

## 802.11T

Исходная цель Рабочей Группы IEEE по Задаче Т [IEEE 802.11 Task Group T (TGT)] была в разработке метрик производительности, способов измерения, и условий тестирования для измерения производительности беспроводного 802.11 сетевого оборудования.



Заглавная *T* в названии *IEEE 802.11T* показывает, что эта поправка считается рекомендуемой практикой, а не стандартом. Поправка 802.11T никогда не была принята и была отменена.

Предлагаемая поправка 802.11T также называлась как *Прогноз Беспроводной Производительности* [*Wireless Performance Prediction (WPP)*]. Ее конечной целью были однозначные и универсальные принятые практики измерения БЛВС. Эти критерии производительности и методы могли бы использоваться независимыми испытательными лабораториями, производителями, и даже конечными пользователями.



### Являются ли Результаты Пропускной Способности Одними и Теми же между Производителями?

Несколько факторов могут повлиять на пропускную способность в беспроводной сети, включая физическую среду, дальность действия, и тип шифрования. Еще один фактор, который может повлиять на пропускную способность - это просто радиоустройство производителя, которое используется для передачи. Даже если стандарт 802.11-2020 четко определяет ширины полос пропускания частоты, скорости передачи данных, и методы доступа к среде, результаты пропускной способности широко варьируются от производителя к производителю. Тест производительности пропускной способности с использованием ТД от одного производителя может дать сильно отличающиеся результаты, от того же самого теста производительности пропускной способности с использованием похожих ТД но от другого производителя. Однако, конкурентные(самые лучшие) результаты пропускной способности обычно не очень реалистичны, потому что они получаются с помощью одного Wi-Fi клиента, подключенного к одной ТД. Многие переменные влияют на пропускную способность в реальном мире, включая число подключенных клиентов, тип клиентов, и используемое приложение. Также, пропускная способность - это только одна из многих существенных метрик производительности Wi-Fi. Например, роуминг, QoS, и безопасность также важны. Глава 13 "Концепции Проектирования БЛВС", и другие главы о пропускной способности этой книги рассматривают многие из этих реальных аспектов. Хотя стандартизованные метрики 802.11T никогда не были приняты, Wi-Fi Альянс определяет свои собственные метрики для нейтральных к производителю лабораторных испытаний для всех сертификаций Wi-Fi Альянса.

## IEEE Группа по Задаче m

Рабочая Группа IEEE по Задаче m [IEEE Task Group m (TGm)] запустила инициативу в 1999 году для внутренней поддержки технической документации стандарта 802.11. 802.11m часто называют как 802.11 домработник/домработница [*802.11 housekeeping*], так как ее миссия в уточнении и корректировке стандарта 802.11. До тех пор, пока вы не являетесь членом TGm, эта поправка имеет небольшое значение. Однако, эта рабочая группа по задаче также отвечает за объединение принятых поправок в публикуемую документацию. Следующий список показывает ревизии стандарта, которые были созданы за несколько лет, вместе с рабочей группой по задаче, ответственной за каждую ревизию.

IEEE Std 802.11-2007	802.11 TGma
IEEE Std 802.11-2012	802.11 TGmb
IEEE Std 802.11-2016	802.11 TGmc
IEEE Std 802.11-2020	802.11 TGmd



Не существует ни поправки 802.11l, ни 802.11o, потому что они считаются типологически проблемными. Поправку 802.11ab пропустили, чтобы избежать путаницы с устройствами, которые используют 802.11a и 802.11b PHY технологии, которые часто называются устройствами 802.11a/b. Поправка 802.11ag была пропущена, чтобы избежать путаницы с устройствами, которые используют 802.11a и 802.11g PHY технологии, и которые называются устройствами 802.11a/g. Также, стоит отметить, что нет поправок с названием 802.11x. Термин 802.11x иногда используется для отсылки ко всем стандартам 802.11. Стандарт IEEE 802.1X, который является стандартом контроля доступа на основе портов, часто некорректно называют 802.11x.

# Итого

Эта глава охватывает исходный стандарт 802.11, поправки, объединенные в стандарт 802.11-2007, стандарт 802.11-2012, стандарт 802.11-2016, и стандарт 802.11-2020, а также черновые поправки 802.11. Мы рассмотрели следующее:

- Все определенные исходным Первичным стандартом 802.11 [802.11 Prime] требования уровней PHY и MAC
- Все утвержденные улучшения к стандарту 802.11 в форме принятых поправок, включая более высокие скорости передачи данных, разные технологии расширения спектра, качество сервиса, и безопасность.
- Будущие возможности и улучшения в качестве предложений черновых документов 802.11

Стандарт 802.11-2020 и все будущие улучшенные добавления обеспечивают очень нужную основу для производителей, сетевых администраторов и конечных пользователей.

Экзамен CWNA проверяет ваши знания стандарта 802.11-2020 и всех относящихся к нему технологий.

## Темы Экзамена

**Знать технологии расширения спектра, определенные в исходном стандарте 802.11 и последующих стандартах 802.11-2007, 802.11-2012, 802.11-2016, и 802.11-2020.** Хотя исходный стандарт 802.11 определяет инфракрасную связь, FHSS, и DSSS, поздние поправки, которые сейчас включены в стандарт 802.11-2020 также определяют HR-DSSS, OFDM, ERP, HT, и VHT.

**Помнить и требуемые скорости передачи данных и поддерживаемые скорости передачи данных для каждого PHY.**

DSSS и FHSS требуют и поддерживают скорости передачи данных в 1 и 2 Мбит/с. Другие PHYs предлагают более широкую поддержку скоростей передачи данных. Например, OFDM и ERP-OFDM поддерживают скорости передачи данных в 6, 9, 12, 18, 24, 36, 48, и 54 Мбит/с, но только скорости 6, 12, и 24 Мбит/с являются обязательными. С введением 802.11n, важно понимать концепцию схем модуляции и кодирования [modulation coding schemes (MCSs)], которые также определены в 802.11ac. Пожалуйста, учите, что скорости передачи данных - это скорости передачи, а не агрегированная пропускная способность.

**Знать полосы частот, используемые каждым PHY, в соответствии с определением стандарта 802.11-2020.**

Оборудование 802.11a и 802.11ac работает в 5 ГГц полосах U-NII. Устройства DSSS, FHSS, HR- DSSS, и ERP (802.11g) передают и принимают в полосе ISM 2.4 ГГц. Нужно понимать, что устройства 802.11n передают в полосах частот 2.4 ГГц или 5 ГГц.

**Определить контроль мощности передачи и динамического выбора частоты.** ТРС и DFS являются обязательными для использования в полосе 5 ГГц. Обе технологии используются в качестве средства для предотвращения интерференции с передачей радара.

**Объяснить определенные стандарты беспроводной безопасности, и pre-802.11i и post-802.11i.**

Before

До перехода на 802.11i, были определены WEP и TKIP. Поправка 802.11i обращается к использованию CCMP/AES для шифрования. Для аутентификации 802.11i определяет или решение 802.1X/EAP или использование аутентификации PSK.

# Контрольные Вопросы

1. Сертификация Wi-Fi HaLow от Wi-Fi Альянса вероятно будет использоваться для сенсорных сетей и устройств Интернета Вещей [Internet of Things (IoT)] и основана на какой поправке IEEE?

  - A.** 802.11aq
  - B.** 802.11ak
  - C.** 802.11ae
  - D.** 802.11ai
  - E.** 802.11ah
2. Какая поправка определяет улучшения производительности с помощью более высокой нелицензируемой полосы частот 60 ГГц, и способом передачи, который называется как направленный мультигигабит [directional multi-gigabit (DMG)]?

  - A.** 802.11ac
  - B.** 802.11ad
  - C.** 802.11ay
  - D.** 802.11q
  - E.** 802.11z
3. Какие типы устройств были определены в исходном стандарте 802.11? (Выберите все, что применимо.)

  - A.** OFDM
  - B.** DSSS
  - C.** HR-DSSS
  - D.** IR
  - E.** FHSS
  - F.** ERP
4. Какая поправка 802.11 определяет механизмы беспроводной взаимносоединяемой [mesh] сетевой работы?

  - A.** 802.11n
  - B.** 802.11u
  - C.** 802.11s
  - D.** 802.11v
  - E.** 802.11k
5. Надежная защищенная сеть [robust security network (RSN)] требует использование каких механизмов безопасности? (Выберите все, что применимо.)

  - A.** 802.11x
  - B.** WEP
  - C.** IPsec
  - D.** CCMP/AES

- E.** CKIP
  - F.** 802.1X
- 6.** Радиомодуль 802.11ac может передавать на какой частоте и использовать какую технологию расширения спектра?
- A.** 5 МГц, OFDM
  - B.** 2.4 ГГц, HR-DSSS
  - C.** 2.4 ГГц, ERP-OFDM
  - D.** 5 ГГц, VHT
  - E.** 5 ГГц, DSSS
- 7.** Какие скорости передачи данных являются требуемыми для станции OFDM?
- A.** 3, 6, и 12 Мбит/с
  - B.** 6, 9, 12, 18, 24, 36, 48, и 54 Мбит/с
  - C.** 6, 12, 24, и 54 Мбит/с
  - D.** 6, 12, и 24 Мбит/с
  - E.** 1, 2, 5.5, и 11 Мбит/с
- 8.** При внедрении 802.1X/EAP RSN сети с решением VoWiFi, что нужно, чтобы избежать проблемы с задержкой при роуминге?
- A.** Протокол Между Точками Доступа [Inter-Access Point Protocol]
  - B.** Быстрый BSS переход [Fast BSS transition]
  - C.** Функция Распределенной Координации [Distributed Coordination Function]
  - D.** Функция Координации Роуминга [Roaming Coordination Function]
  - E.** Легковесная ТД [Lightweight APs]
- 9.** Какие технологии дебютировали в поправке 802.11ac-2013? (Выберите все, что применимо.)
- A.** MIMO
  - B.** MU-MIMO
  - C.** 256-QAM
  - D.** 40 МГц каналы
  - E.** 80 МГц каналы
- 10.** Частоты телевизионного белого пространства [TV white space (TVWS)] работающие между 54 МГц и 790 МГц, используют новый PHY, который называется как TVHT, и определен какой поправкой 802.11?
- A.** 802.11af
  - B.** 802.11y
  - C.** 802.11a
  - D.** 802.11aa
  - E.** 802.11ad

- 11.** Какие две технологии используются для предотвращения радиомодулей 802.11 от интерферирования с радаром и спутниковой передачей на 5 ГГц?
- A.** Динамический Выбор Частоты [Dynamic frequency selection]
  - B.** Улучшенный Распределенный Канальный Доступ [Enhanced Distributed Channel Access]
  - C.** Расширение Спектра Прямой Последовательностью [Direct-sequence spread-spectrum]
  - D.** Протокол Целостности Временного Ключа [Temporal Key Integrity Protocol]
  - E.** Контроль Мощности Передачи [Transmit power control]
- 12.** Какие поправки 802.11 обеспечивают пропускную способность в 1 Гбит/с и выше? (Выберите все, что применимо.)
- A.** 802.11aa
  - B.** 802.11ab
  - C.** 802.11ac
  - D.** 802.11ad
  - E.** 802.11ae
  - F.** 802.11af
- 13.** В соответствии с определением стандарта 802.11-2020, какое оборудование совместимо? (Выберите все, что применимо.)
- A.** ERP и HR-DSSS
  - B.** HR-DSSS и FHSS
  - C.** VHT и OFDM
  - D.** 802.11h и 802.11a
  - E.** HR-DSSS и DSSS
- 14.** Какая максимальная скорость передачи данных определена поправкой 802.11ac?
- A.** 54 Мбит/с
  - B.** 1300 Мбит/с
  - C.** 3466.7 Мбит/с
  - D.** 6933.3 Мбит/с
  - E.** 60 Гбит/с
- 15.** Что является доступными опциями безопасности, согласно определению исходного стандарта IEEE Std 802.11-1999 (R2003)? (Выберите все, что применимо.)
- A.** CCMP/AES
  - B.** Аутентификация Открытой Системы [Open System authentication]
  - C.** Предварительно известные общие ключи [Preshared keys]
  - D.** Аутентификация с Общим Ключом [Shared Key authentication]
  - E.** WEP
  - F.** TKIP

- 16.** Поправка 802.11u-2011 также как называется?
- A.** WIEN (Wireless Interworking with External Networks) - Беспроводная Межсетевая Работа с Внешними Сетями
  - B.** WLAN (wireless local area networking) - Беспроводная Локальная Вычислительная Сеть
  - C.** WPP (Wireless Performance Prediction) Прогноз Беспроводной Производительности
  - D.** WAVE (Wireless Access in Vehicular Environments) Беспроводной Доступ в Транспортных Средах
  - E.** WAP (Wireless Access Protocol) - Протокол Беспроводного Доступа
- 17.** Стандарт 802.11-2020 определяет какие две технологии для качества-сервиса [quality of service (QoS)] в БЛВС?
- A.** EDCA
  - B.** PCF
  - C.** Канальный Доступ, Контролируемый Функцией Гибридной Координации [Hybrid Coordination Function Controlled Channel Access]
  - D.** VoIP
  - E.** Функция Распределенной Координации [Distributed Coordination Function]
  - F.** VoWiFi
- 18.** Поправка 802.11h (теперь часть стандарта 802.11-2020) ввела какие два главных изменения для 5 ГГц радиомодулей?
- A.** TPC
  - B.** IAPP
  - C.** DFS
  - D.** DMG
  - E.** FHSS
- 19.** Поправка 802.11n определила какой PHY?
- A.** HR-DSSS
  - B.** FHSS
  - C.** OFDM
  - D.** PBCC
  - E.** HT
  - F.** VHT
- 20.** Какие уровни модели OSI затрагиваются в стандарте 802.11? (Выберите все, что применимо.)
- A.** Прикладной [Application]
  - B.** Канальный [Data-Link]
  - C.** Презентационный [Presentation]
  - D.** Физический [Physical]
  - E.** Транспортный [Transport]
  - F.** Сетевой [Network]



# Глава

# 3

# Основы РадиоТехники

**В ЭТОЙ ГЛАВЕ, ВЫ УЗНАЕТЕ СЛЕДУЮЩЕЕ:**

✓ Что такое радиочастотный сигнал (радиосигнал)

✓ Характеристики радиоволн

- Длина волны
- Частота
- Амплитуда
- Фаза

✓ Поведение радиоволн

- Распространение волн
- Поглощение
- Отражение
- Рассеивание
- Рефракция
- Дифракция
- Потери (затухание)
- Ослабление в свободном пространстве
- Многолучевое распространение
- Усиление
- Радиоизмерительные инструменты



В дополнение к пониманию модели OSI и базовым сетевым концепциям, вы должны расширить ваше понимание множества других сетевых технологий для того,

чтобы правильно проектировать, устанавливать и администрировать беспроводные сети 802.11. Например, при администрировании сети Ethernet, вам обычно нужно понимание TCP/IP, мостов [bridge], коммутации, и маршрутизации. Навыки управления сетью Ethernet также поможет вам как администратору беспроводной ЛВС (БЛВС), потому что большинство беспроводных сетей 802.11 действуют как "порталы" в проводные сети. IEEE определяет связь 802.11 на физическом уровне и MAC подуровне канального [Data-Link] уровня.

Чтобы полностью понять технологию 802.11, вам нужно иметь ясную концепцию того, как работает беспроводная связь на первом уровне модели OSI, а в сердце Физического уровня - это радиосвязь.

В проводной ЛВС, сигнал заключен точно внутри провода, а результирующее поведение предсказуемо. Однако, для БЛВС верно обратное. Хотя законы физики выполняются, радиосигнал проходит через пространство иногда непредсказуемым способом. Так как радиосигнал не находится в Ethernet проводе, вам стоит всегда пытаться представлять БЛВС как "постоянно меняющуюся" сеть.

Означает ли это, что вы должны быть радиоинженером из Стэнфордского Университета, чтобы провести обследование БЛВС или мониторить сеть Wi-Fi? Конечно нет! Но вы должны иметь хорошее понимание характеристик радиоволн и их поведение, описанные в этой главе, чтобы ваши навыки, в качестве администратора беспроводной сети продвинулись на новый уровень. Почему беспроводная сеть работает по-разному в аудитории полной людей, нежели чем в пустой аудитории? Почему эффективная дальность действия 5ГГц радиопередатчика короче дальности действия радиопередатчика 2,4ГГц? На такие типы вопросов можно ответить, обладая некоторыми базовыми знаниями того, как работают и действуют радиосигналы.



Проводная связь проходит через так называемую *ограниченную среду*. Ограниченная среда содержит в себе или ограничивает сигнал (хотя небольшое количество утечки сигнала происходит) Беспроводная связь проходит через так называемую *неограниченную среду*. Неограниченная среда не держит сигнал, который излучается в окружающую среду во всех направлениях (до тех пор, пока не ограничена или не перенаправлена некоторым внешним воздействием).

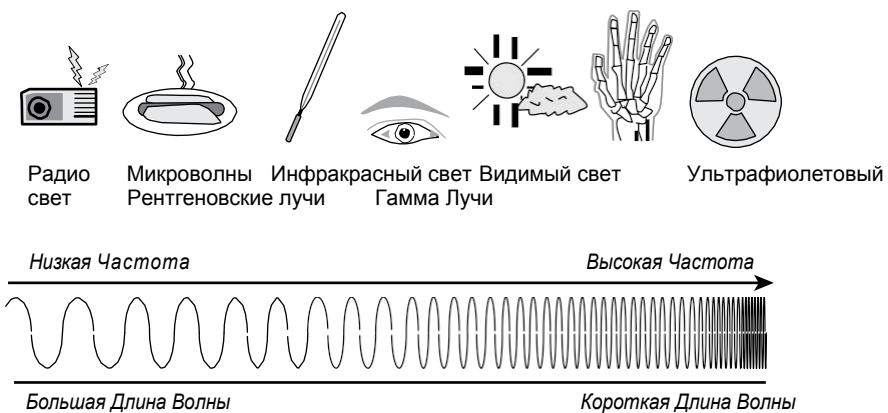
В этой главе мы сначала определим из чего состоит радиосигнал, а затем мы обсудим и свойства и поведение радиоволн.

# Что такое радиосигнал?

Эта книга ни в коем случае не претендует на роль исчерпывающего руководства по законам физики, которая является наукой о движении и материи. Однако, базовое понимание некоторых концепций физики, связанных с радиоволнами важно даже для профессионала по беспроводным сетям начального уровня.

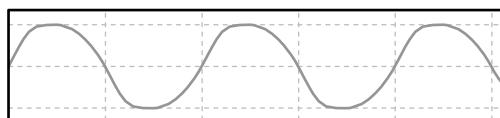
*Электромагнитный спектр*, который обычно просто называют спектр, это диапазон всех возможных электромагнитных излучений. Это излучение существует в виде самораспространяющихся электромагнитных волн, которые могут перемещаться через материю или пространство. Примеры электромагнитных волн включают: гамма лучи, рентгеновские лучи, видимый свет, и радиоволны. Радиоволны - это электромагнитные волны, возникающие в радиоволновой части электромагнитного спектра, как показано на Рисунке 3.1.

**РИСУНОК 3.1** Электромагнитный спектр



Радиосигнал начинается как сигнал электрического *переменного тока*, генерируемого источником. Этот сигнал переменного тока передается по медному проводнику (обычно коаксиальному кабелю), и излучается антенным элементом в виде электромагнитной волны. Эта электромагнитная волна и есть беспроводной сигнал. Изменения электронного потока в антenne, по-другому называется *током*, вызывает изменения в электромагнитных полях вокруг антеннны.

Переменный ток - это электрический ток, величина и направление которого изменяются циклически, в отличие от постоянного тока, направление которого остается неизменным. Вид и форма сигнала переменного тока - определяемые как *Волновая форма* или *Форма сигнала [Waveform]* - это то, что называется, как *синусоидальная волна*, как показано на Рисунке 3.2. Формы синусоидальной волны можно встретить в свете, звуке и океане. Изменение напряжения переменного тока называется, как *периодичность(цикличность)* или как *осцилляция(колебание)*.

**РИСУНОК 3.2** Синусоидальная волна

Радиочастотный электромагнитный сигнал излучается в непрерывной форме, которая определяется конкретными свойствами, такими как длина волны, частота, амплитуда и фаза. Кроме того, электромагнитные сигналы могут проходить через среды из различных материалов или абсолютный вакуум. Когда радиосигнал проходит сквозь вакуум, он движется со скоростью света, которая составляет 299 793 458 метров в секунду (м/с) или 186 282 мили в секунду.



Чтобы упростить математические вычисления, которые используют скорость света, в общем случае округляют значение до 300 000 000 метров в секунду или округляют до 186 000 миль в секунду. Любая ссылка на скорость света в этой книге будет использовать округленное значение.

Электромагнитный радиосигнал распространяется с различным или комбинированным поведением движения. Это поведение движения называется *видом распространения*. Мы обсудим некоторые из этих видов распространения, включая поглощение, отражение, рассеяние, рефракцию, дифракцию, усиление и затухание - позже в этой главе.

## Характеристики Радиоволн

Следующие характеристики, определяемые законами физики, присутствуют в каждом радиосигнале:

- Длина волны
- Частота
- Амплитуда
- Фаза

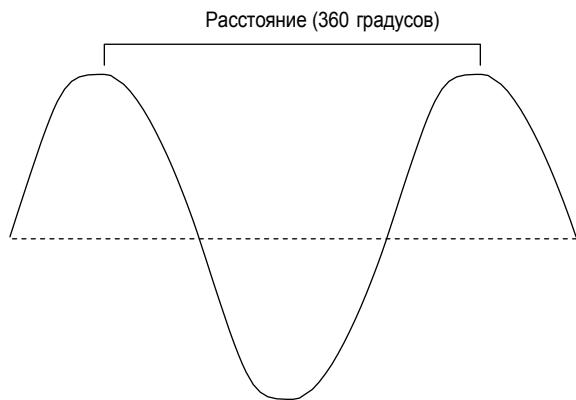
Вы рассмотрите каждую из них более подробно в следующих разделах.

### Длина волны

Как сказано ранее, радиосигнал — это переменный ток, который непрерывно изменяется между положительным и отрицательным напряжением. Колебание, или период этого переменного тока определяется как разовое изменение верх-вниз-верх, или изменение от положительного к отрицательному, и затем снова к положительному.

*Длина волны* - это расстояние между двумя следующими друг за другом гребнями (пиками) или двумя следующими друг за другом впадинами (долинами) волны, как показано на Рисунке 3.3. Простыми словами, длина волны это расстояние, которое в реальности занимает один период (цикл) радиосигнала.

**РИСУНОК 3.3** Длина волны



Хотя физически длина волны может быть различной, о чем вы скоро узнаете, волны имеют сходные относительные свойства и одинаково измеряются. Каждая волна измеряется от пика до пика, и каждая имеет впадину между пиками. Относительное измерение называется *градусы*, используется для обозначения различных точек на этом участке. Как показано на Рисунке 3.3, расстояние целой волны, от пика до пика, составляет 360 градусов. Впадина находится на 180 градусе. Первая точка, где волна пересекает горизонтальную линию, это 90 градусов, а вторая точка, где она пересекает горизонтальную линию - это 270 градусов. Вам не нужно будет иметь дело с градусами, за исключением понимания концепции фазы позже в этой главе.

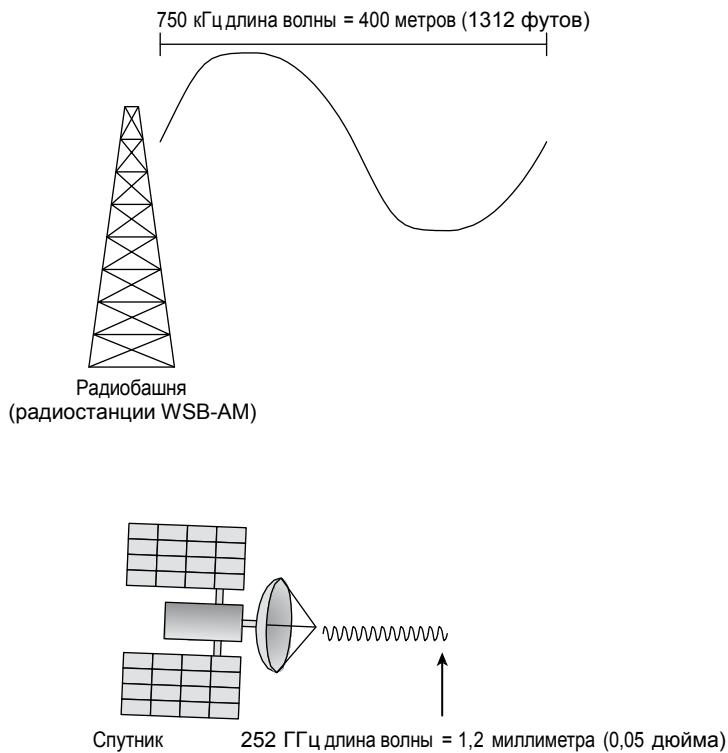


Греческий символ  $\lambda$  (лямбда) обозначает длину волны. Частота обычно обозначается Латинской буквой  $f$ . Латинская буква с обозначает скорость света в вакууме. Оно получено от *celeritas*, Латинское слово означающее скорость.

Очень важно понимать, что существует обратная зависимость между длиной волны и частотой. Три компонента этой обратной зависимости - это частота ( $f$ , измеряемая в герцах, Гц), длина волны ( $\lambda$ , измеряемая в метрах, или м.), и скорость света ( $c$ , которая является постоянным значением 300 000 000 м/с). Следующая справочная формула иллюстрирует это отношение:  $\lambda=c/f$  и  $f=c/\lambda$ . Упрощенное объяснение это, что чем выше частота радиосигнала, тем меньше длина волны этого сигнала. Чем больше длина волны радиосигнала, тем меньше частота этого сигнала.

**Р И С У Н О К 3 . 4**

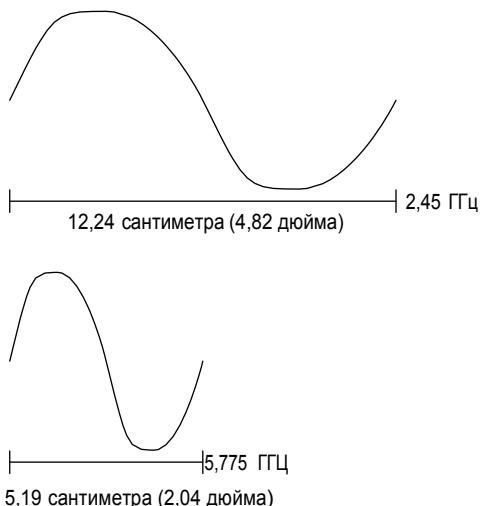
Длина волны 750кГц и длина волны 252ГГц



AM-радиостанции работают на гораздо более низких частотах, чем радиомодули BLVS 802.11, тогда как спутниковые радиопередачи осуществляются на гораздо более высоких частотах, чем радиомодули BLVS. Например, радиостанция WSB-AM в Атланте вещает на 750 кГц и имеет длину волны 400 метров или 1312 футов. Это довольно большое расстояние для прохождения одного периода радиосигнала. Наоборот, некоторые радионавигационные спутники работают на очень высокой частоте, около 252 ГГц, и один период спутникового сигнала имеет длину волны менее 1,2 миллиметра или 0,05 дюйма. Рисунок 3.4 показывает сравнение этих двух совершенно разных типов радиосигналов.

Когда радиосигналы проходят через пространство и материю, они теряют силу сигнала (затухают). Часто считается, что высокочастотный электромагнитный сигнал с меньшей длиной волны будет затухать быстрее, чем низкочастотный сигнал с большей длиной волны. В действительности, свойства радиосигнала: частота и длина волны, не являются причиной затухания. Расстояние является основной причиной затухания. Все антенны имеют эффективную площадь для приема мощности, которая называется *апертура*. Количество радиоволновой энергии, которое может быть собрано апертурой антенны меньше у высокочастотных антенн. И хотя длина волны и частота не являются причиной затухания, считается, что более высокочастотные сигналы с меньшей длиной волны затухают быстрее, чем сигналы с большей длиной волны. Теоретически в вакууме электромагнитные сигналы будут путешествовать вечно. Однако по мере того, как сигнал проходит через нашу атмосферу, сигнал будет затухать до амплитуд ниже порога чувствительности приема принимающей радиостанции. Фактически, сигнал придет к приемнику, но он будет слишком слабым, чтобы его можно было обнаружить.

**РИСУНОК 3.5** 2,45 ГГц длина волны и 5,775 ГГц длина волны



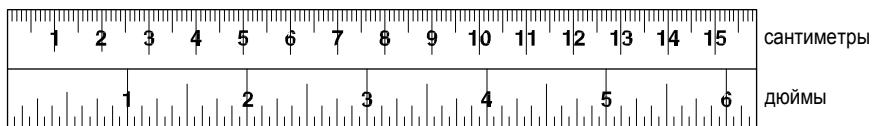
Считается, что высокочастотный сигнал с меньшей длиной волны не будет распространяться так же далеко, как низкочастотный сигнал с большей длиной волны. Реальность такова, что количество энергии, которое может быть собрано апертурой высокочастотной антенны, меньше, чем количество радиоволновой энергии, которое может быть собрано низкочастотной антенной. Хорошой

аналогией принимающей радиостанции может быть человеческое ухо. В следующий раз, когда вы услышите, как машина едет по улице с громкой музыкой, обратите внимание, что первым, что вы услышите, будут басы (низкие частоты). Этот практический пример демонстрирует, что низкочастотный сигнал с большей длиной волны будет слышен на большем расстоянии, чем более высокочастотный сигнал с меньшей длиной волны.

Большинство радиомодулей БЛВС работают или в диапазоне частот 2,4 ГГц, или в диапазоне 5 ГГц. На Рисунке 3.5 вы видите сравнение одного периода двух волн, генерируемых двумя радиомодулями БЛВС, каждая из которых передает в разных полосах частот.

Высокочастотные сигналы, в основном, затухают быстрее, чем низкочастотные сигналы, когда они проходят через различные физические среды, такие как кирпичные стены. Это важно знать инженеру беспроводной связи по двум причинам. Первая, дальность покрытия зависит от затухания в воздухе (называется затуханием в свободном пространстве, обсуждается далее в этой главе). Вторая, чем выше частота, тем, обычно, меньше сигнал будет проникать через препятствия. Например, 2,4 ГГц сигнал будет проходить через стены, окна и двери с большей амплитудой, чем сигнал на частоте 5 ГГц. Подумайте, насколько дальше вы можете принимать сигнал АМ-станции (более низкая частота) по сравнению с сигналом FM-станции (более высокая частота). Как вы можете видеть на рисунках 3.4 и 3.5, длины волн сигналов различных частот различны, потому что, хотя каждый сигнал повторяется только один раз, волны проходят не одинаковые расстояния. На рисунке 3.6 показан другой способ увидеть разницу в длинах волн радиосигнала, используемого в четырех различных полосах частот, где может использоваться технология Wi-Fi.

**РИСУНОК 3.6** Длины волн сигналов с частотами 2.4 ГГц, 5 ГГц, 6 ГГц, и 60 ГГц



2.437 ГГц (Канал 6)

Длина волны = 12.3 см (4.85 дюйма)

5.500 ГГц (Канал 100)

Длина волны = 5.45 см (2.15 дюйма)

6.675 ГГц (Канал 145)

Длина волны = 4.49 см (1.77 дюйма)

60 ГГц (Канал 3)

Длина волны = 5 мм (0.2 дюйма)



Обратите внимание, что длина волны 2,45 ГГц составляет около 4,8 дюйма или 12 сантиметров. Длина волны 5,775 ГГц составляет всего около 2 дюймов или 5 сантиметров..

Как вы можете видеть на рисунках 3.4, 3.5 и 3.6, длины волн различных частотных сигналов различны, потому что, хотя каждый сигнал повторяется только один раз, волны проходят неодинаковые расстояния. На рис. 3.7 вы видите формулы для расчета

длины волны в дюймах или сантиметрах.

### РИСУНОК 3.7 Формулы длины волны

$$\text{Длина волны (дюймы)} = 11,811/\text{частота (ГГц)}$$

$$\text{Длина волны (сантиметры)} = 30/\text{частота (ГГц)}$$



В этом учебном пособии вам будут представлены различные формулы. Вам не нужно знать эти формулы для сертификационного экзамена CWNA. Формулы приведены в этом учебном пособии для демонстрации концепций и для использования в качестве справочного материала.



### Реальный Сценарий

#### Как Длина Волны Сигнала Касается Меня?

Часто считается, что высокочастотный электромагнитный сигнал с меньшей длиной волны будет затухать быстрее, чем низкочастотный сигнал с большей длиной волны. В действительности свойства радиосигнала: частота и длина волны не вызывают затухания.. Расстояние является основной причиной затухания. Все антенны имеют эффективную площадь для приема мощности, которая называется как апертура. Количество радиоволновой энергии, которое может быть собрано апертурой антенны меньше у высокочастотных антенн. И хотя длина волны и частота не являются причиной затухания, считается, что более высокочастотные сигналы с меньшей длиной волны затухают быстрее, чем сигналы с большей длиной волны. Когда все остальные аспекты беспроводного канала связи аналогичны, оборудование Wi-Fi, использующее радиочастоты 5 ГГц и 6 ГГц, будет иметь более короткую фактическую дальность действия и меньшую зону покрытия, чем оборудование Wi-Fi, использующее радиочастоты 2,4 ГГц.

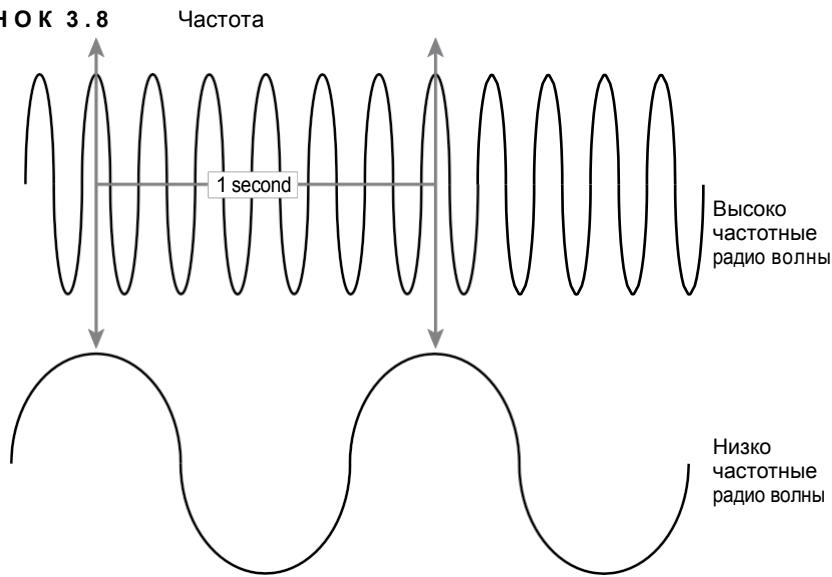
Часть проекта БЛВС включает в себя то, что называется *обследованием объекта (site survey)* или *радиообследованием*. Главным аспектом обследования объекта является подтверждение зон или сот покрытия в ваших зданиях пригодными для использования принимаемого сигнала. Если точки доступа с одночастотным радиомодулем, то точки доступа 2,4 ГГц обычно могут обеспечить большую зону радиопокрытия для клиентских станций, чем высокочастотное оборудование. Потребуется установить больше точек доступа с частотой 5 ГГц, чтобы обеспечить такое же покрытие, которое может быть достигнуто за счет меньшего количества точек доступа с частотой 2,4 ГГц. Способность проникновения таких сигналов также значительно уменьшает покрытие для 5 ГГц, нежели чем для 2,4 ГГц. Большинство производителей корпоративного Wi-Fi продают двухчастотные точки доступа (ТД) с 2,4 ГГц и 5 ГГц радиомодулями. Планирование обследования объекта и анализ покрытия для двухчастотных точек доступа должны изначально основываться на более высокочастотном 5 ГГц сигнале, который фактически обеспечивает меньшую зону покрытия. В ближайшем будущем, производители Wi-Fi будут продавать трехчастотные ТД с 2,4 ГГц, 5 ГГц, и 6 ГГц радиомодулями. (На момент

перевода уже продают). В качестве заметки на полях: проектирование БЛВС(WLAN) включает в себя гораздо больше, чем просто планирование покрытия. Планирование клиентской емкости и потребления эфирного времени так же важно, как и проектирование покрытия. Эти приемы проектирования подробно описаны в главе 13 «Концепции проектирования БЛВС(WLAN)».

## Частота

Как упоминалось ранее, Радиосигнал совершает периодические колебания в переменном токе в форме электромагнитной волны. Вы также знаете, что расстояние, пройденное за один цикл(период) сигнала, равно длине волны. Но как насчет того, как часто Радиосигнал повторяется в определенный период времени? *Частота* это количество раз, когда определенное событие происходит в течение заданного интервала времени. Стандартным измерением частоты является герц (Гц), названный в честь немецкого физика Генриха Рудольфа Герца. Событие, происходящее раз в 1 секунду, имеет частоту 1 Гц. Событие, которое происходит 325 раз за 1 секунду, измеряется как 325 Гц. Частота при которой электромагнитная волна осуществляет периодические колебания также измеряется в герцах. Таким образом, количество колебаний, которое радиосигнал сделает за 1 секунду является частотой этого сигнала, как показано на Рисунке 3.8.

**РИСУНОК 3.8**



Различные метрические приставки могут быть применены к герцам при измерении радиочастоты, чтобы сделать работу с очень большими частотами проще:

1 герц (Гц) = 1 период (цикл) в секунду

1 килогерц (кГц) = 1 000 периодов (циклов) в секунду

1 мегагерц (МГц) = 1 000 000 (миллион) периодов (циклов) в секунду

1 гигагерц (ГГц) = 1 000 000 000 (миллиард) периодов (циклов) в секунду

Так, когда мы говорим о 5 ГГц Wi-Fi радио, радиосигнал колеблется 5 миллиардов раз в секунду!

## Обратная зависимость

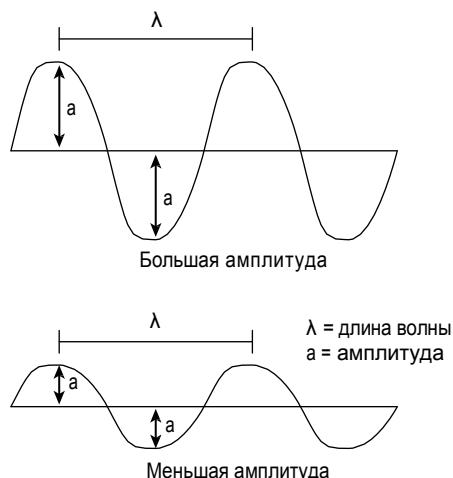
Помните, что существует обратная зависимость между длиной волны и частотой.. Три компонента этой обратной зависимости - это частота ( $f$ , измеряемая в герцах, Гц), длина волны ( $\lambda$ , измеряемая в метрах , или м.), и скорость света ( $c$ , которая является постоянным значением 300 000 000 м/с). Следующая справочная формула иллюстрирует это отношение:  $\lambda=c/f$  и  $f=c/\lambda$ . Упрощенное объяснение это, что чем выше частота радиосигнала, тем меньше длина волны этого сигнала. Чем больше длина волны радиосигнала, тем меньше частота этого сигнала.

## Амплитуда

Еще одним очень важным свойством радиосигнала является амплитуда, которую можно охарактеризовать просто как силу сигнала или мощность. Когда говоря о беспроводной передаче, часто говорят о том насколько громким или сильным является сигнал. Амплитуду можно определить как максимальное смещение непрерывной волны. В радиосигналах амплитуда соответствует электрическому полю волны.. Когда вы смотрите на радиосигнал с помощью осциллографа, амплитуда представлена положительными гребнями и отрицательными впадинами синусоиды.

На Рисунке 3.9, вы можете увидеть, что  $\lambda$  представляет длину волны , и  $a$  представляет амплитуду. Гребни и впадины первого сигнала имеют большую величину; таким образом, сигнал имеет большую амплитуду. Гребни и впадины второго сигнала имеют меньшую амплитуду, поэтому сигнал имеет меньшую амплитуду.

**Р И С У Н О К 3 . 9** Амплитуда





Хотя сила сигнала (амплитуда) различная, частота и длина волны сигнала остается постоянной. Ряд факторов может привести радиосигнал к уменьшению амплитуды, это также называется как **затухание или аттенюация [attenuation]**, которую мы обсудим позже в этой главе, в разделе "Потери (Затухание)".

При обсуждении мощности сигнала в БЛВС под амплитудой обычно понимают либо амплитуду передачи, либо амплитуду приема. Амплитуда передачи обычно определяется как величина начальной амплитуды, которая покидает радиопередатчик. Например, если вы настроите точку доступа для передачи на уровне 15 милливатт (мВт), то это будет амплитуда передачи. Кабели и разъемы ослабляют амплитуду передачи, в то время как большинство антенн усиливают амплитуду передачи. Когда радиомодуль принимает радиосигнал, мощность принятого сигнала чаще всего называют *принимаемой амплитудой (или амплитудой приема)*. Измерение силы радиосигнала, выполненное во время контрольного радиообследования, является примером принимаемой амплитуды.

Различные типы радиотехнологий требуют амплитуды передачи разной степени. АМ радиостанции могут передавать узкополосный сигнал с мощностью 50 000 ватт (Вт). Радиопередатчики, используемые в большинстве внутренних точках доступа 802.11, имеют диапазон мощности передачи между 1 мВт и 100 мВт.

Из других глав вы узнаете, что радиомодули Wi-Fi могут принимать и демодулировать сигналы с амплитудой всего лишь миллиардные доли милливатт.

## Фаза

Фаза не является свойством только одного радиосигнала, а вместо этого включает взаимосвязь между двумя или более сигналами, использующими одну и ту же частоту. Фаза включает соотношение между положением гребней и впадин амплитуд двух сигналов (волновых форм).

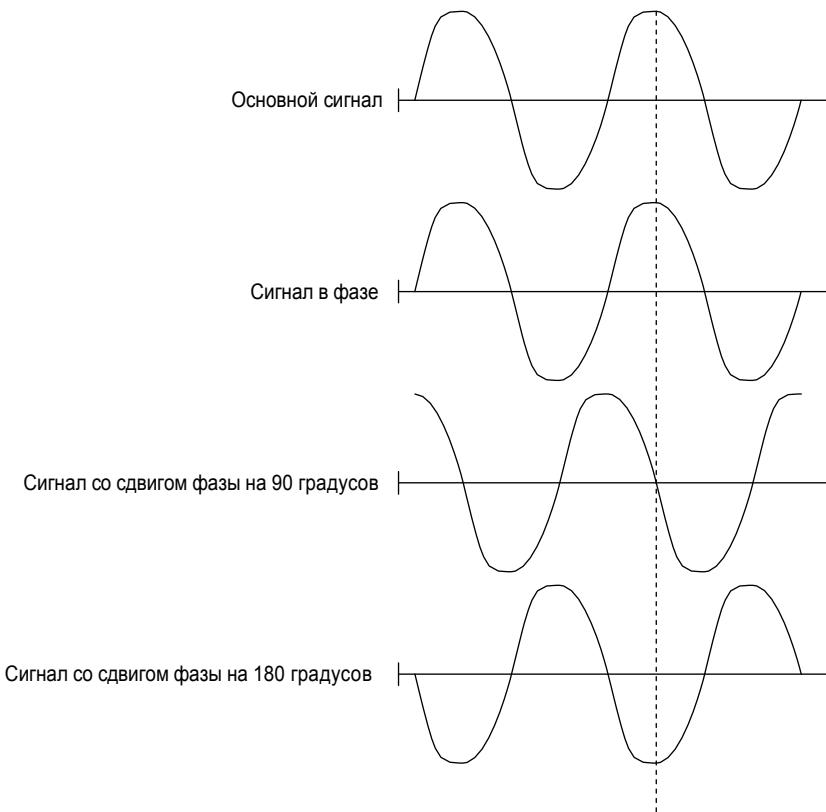
Фаза может измеряться расстоянием, временем или градусами. Если пики двух сигналов с одинаковой частотой находятся в точном соответствии друг с другом в одно и то же время, говорят, что они находятся в *фазе [in phase]*. И наоборот, если пики двух сигналов с одинаковой частотой не совпадают в одно и то же время, говорят, что они *не в фазе [out of phase]*. Рисунок 3.10 иллюстрирует эту концепцию.

Что важно понимать – так это влияние фазы на амплитуду, когда радио принимает несколько сигналов. Сигналы с фазовой разницей в 0 (ноль) градусов фактически складывают свои амплитуды, что приводит к получению сигнала с гораздо большей силой сигнала, потенциально в два раза превышающей амплитуду. Если два радиосигнала сдвинуты по фазе на 180 градусов (пик одного сигнала точно совпадает с впадиной второго сигнала), они компенсируют друг друга, и фактическая мощность принимаемого сигнала равна нулю. Разделение фаз имеет кумулятивный эффект. В зависимости от степени фазового разделения двух сигналов мощность принимаемого сигнала может быть либо увеличена, либо уменьшена. Разность фаз между двумя сигналами является центральной в понимании эффектов радиоволнового явления, известного как многолучевое распространение [multipath], которое обсуждается далее в этой главе.



Андраш Силадьи(András Szilágyi) поддерживает веб-приложение EMANIM для интерактивной визуализации электромагнитных волн. EMANIM позволяет вам манипулировать свойствами волны и видеть последствия изменений. Не забудьте и проверьте EMANIM по адресу <https://emanim.szialab.org/index.html>.

**Р И С У Н О К 3 . 1 0** Взаимосвязь фаз



## Поведение Радиоволн

По мере распространения радиосигнала через воздух и другие среды, он может двигаться и вести себя разными способами. Поведение распространения радиоволны включает: поглощение, отражение, рассеяние, преломление (рефракцию), дифракцию, затухание в свободном пространстве, многолучевое распространение, затухание и усиление. Следующие разделы описывают эти типы поведения.

## Распространение Волн

Теперь, когда вы узнали о некоторых разнообразных характеристиках радиосигнала, важно понять, как ведет себя радиосигнал при движении от антенны. Как было сказано ранее, электромагнитные волны могут двигаться через абсолютный вакуум или проходить через материалы различных сред. Способ, которым двигаются радиоволны называется как распространение волны, – может радикально различаться в зависимости от материалов на

пути сигнала, например: гипсокартон будет иметь совершенно другой эффект на радиосигнал нежели чем металл или бетон.

То, что происходит с радиосигналом между двумя точками, является прямым результатом того как распространяется сигнал. Когда мы используем термин *распространение*, попытайтесь представить радиосигнал расширяющийся или растягивающийся по мере его удаления от антенны. Прекрасная аналогия показана на Рисунке 3.11, на котором изображено землетрясение. Обратите внимание на концентрические сейсмические кольца, которые распространяются от эпицентра землетрясения. Возле эпицентра волны сильные и концентрированные, но по мере удаления сейсмических волн от эпицентра, волны расширяются и ослабевают. Радиоволны ведут себя во многом в такой же манере. Манера в которой перемещается беспроводной сигнал часто называется *особенностью распространения радиоволн [propagation behavior]*.

**Р И С У Н О К 3.11**      Аналогия распространения



Как инженер БЛВС, вы должны понимать особенности распространения радиоволн, чтобы быть уверенным, что точки доступа установлены в правильных местах, чтобы быть уверенным, что выбран правильный тип антенн, а также для мониторинга производительности беспроводной сети.

## Поглощение

Наиболее распространенным поведением радиоволн является *поглощение*. Если сигнал не отражается от объекта, не огибает объект, не проходит через объект, то произошло 100 процентное поглощение. Большинство материалов поглощают некоторое количество радиосигнала в разной степени.

Кирпичные и бетонные стены значительно поглощают сигнал, тогда как гипсокартон поглощает сигнал в меньшей степени. Сигнал на 2.4 ГГц будет иметь 1/16 начальной мощности после прохождения через бетонную стену. Тот же самый сигнал потеряет только половину мощности исходного сигнала после прохождения через гипсокартон. Вода — еще один пример среди, способной в значительной степени

поглощать сигнал. Поглощение является основной причиной затухания (потерь), которое обсуждается далее в этой главе. Объекты, содержащие большое количество воды, такие как аквариумы, мокрая бумага или картон, будут поглощать больше радиоволновой энергии. Амплитуда радиосигнала напрямую зависит от того, сколько радиоволновой энергии поглощается.



## Пример из Реальной Жизни

### Плотность Пользователей

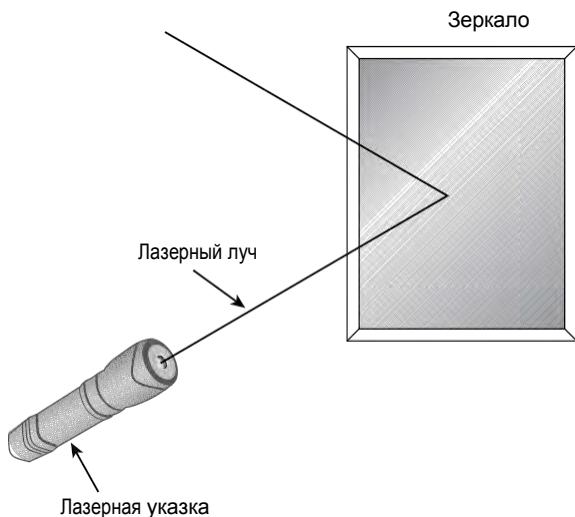
Джон Барретт (John Barrett) провел радиообследование терминала аэропорта. Он определил сколько потребуется точек доступа и их наилучше место размещения, так чтобы он мог получить необходимое радиопокрытие. Десять дней спустя, во время снежного шторма, терминал был переполнен людьми, которые задерживались из-за погоды. Во время этих задержек, сила сигнала и качество БЛВС было ниже желаемого в некоторых местах аэропорта. В чем дело? Человеческие тела!

Среднее взрослое тело это 50 - 65 процентов воды. Вода является причиной поглощения, которое приводит к затуханию. Плотность пользователей является важным фактором при проектировании беспроводной сети. Одна причина это эффект поглощения. Другая причина - это планирование емкости потребления эфирного времени, которое мы обсудим в Главе 13.

## Отражение

Одно из самых важных свойств распространения радиоволн, которые нужно знать — это отражение. Когда волна ударяется о гладкий объект, который больше чем сама волна, то в зависимости от среды волна может отскочить в другом направлении. Такое поведение классифицируется как *отражение*. Аналогичная ситуация может быть, когда ребенок кидает мячик на дорожку и мячик меняет направление. Рисунок 3.12 показывает другую аналогию, лазерный луч направленный на одно небольшое зеркало. В зависимости от угла зеркала, лазерный луч отскакивает или отражается в разных направлениях. Радиосигналы могут отражаться точно таким же способом в зависимости от объектов или материалов, с которыми встречаются сигналы.

Существует два основных типа отражения: *ионосферное отражение [sky wave reflection]* и *микроволновое отражение [microwave reflection]*. Ионосферное отражение может происходить на частотах ниже 1 ГГц, когда сигнал имеет очень большую длину волны. Сигнал отскакивает от поверхности заряженных частиц ионосферы в земной атмосфере. Вот почему вы можете быть в Шарлотте, Северная Каролина, и слушать радиостанцию WLS-AM из Чикаго ясной ночью.

**РИСУНОК 3.12** Аналогия отражения

Микроволновые сигналы, однако, существуют между 1ГГц и 300ГГц. Так как они являются высокочастотными сигналами, у них намного меньшая длина волны, поэтому используется термин – *микроволна [microwave]*. Микроволны могут отражаться от небольших объектов, таких как металлическая дверь. Микроволновое отражение это то, что нас волнует в Wi-Fi среде. На улице микроволны могут отражаться от больших объектов и гладких поверхностей, таких как здания, дороги, водные поверхности, и даже от земной поверхности. Внутри помещений микроволны отражаются от гладких поверхностей, таких как двери, стены и шкафы для документов. Все, что сделано из металла будет абсолютно вызывать отражение. Другие материалы, такие как стекло, бетон, могут также вызывать отражение.

### Каково влияние отражения?

Отражение может быть причиной серьёзных проблем производительности при передаче устаревшего 802.11a/b/g. По мере удаления волны от антенны, она расширяется и рассеивается. Если части этой волны отразятся, появятся новые волновые фронты из точек отражения. Если все это множество волн достигнет приемника, множество отраженных сигналов вызовет эффект, называемый *многолучевое распространение [multipath]*.

Многолучевое распространение может ухудшить силу и качество принимаемого сигнала, или даже вызвать повреждение данных или пропадание сигналов. (Дальнейшее обсуждение многолучевого распространения будет далее в этой главе. Аппаратные решения по компенсации негативного влияния многолучевого распространения в этой среде, такие как направленные антенны и антеннное разнесение, обсуждаются в Главе 5 «Радиосигнал и Концепции антенн»)

Отражение и многолучевое распространение часто рассматриваются как основные враги при развертывании устаревших радиосетей 802.11a/b/g. Радиомодули 802.11n и 802.11ac используют антенны *Много-Вводов, Много-Выходов (multiple-input, multiple-output)*

## Рассеивание

Знали ли вы что цвет неба голубой потому, что молекулы атмосферы меньше, чем длина волны света? Этот явление голубого неба известно как *Релеевское рассеивание* (названного в честь Британского физика 19ого века Джона Уильяма Стретта, Лорда Релея [John William Strutt, Lord Rayleigh]). Более короткие голубые длины волн света поглощаются газами в атмосфере и излучаются во всех направлениях. Этот пример поведения распространения радиоволн называется *рассеивание [scattering]*.

Рассеивание можно наиболее просто описать как множественные отражения. Эти множественные отражения происходят, когда длина волны электромагнитного сигнала больше, чем частицы какой бы то ни было среды, от которой сигнал отражается или через которую проходит.

Рассеивание может происходить двумя способами. Первый тип рассеивания происходит на низком уровне и имеет меньшее влияние на качество и силу сигнала. Этот тип рассеивания может проявляться, когда радиосигнал проходит через вещество, а отдельные электромагнитные волны отражаются от мельчайших частиц в среде. Смог в нашей атмосфере и песчаные бури в пустынях могут вызывать такой тип рассеивания.

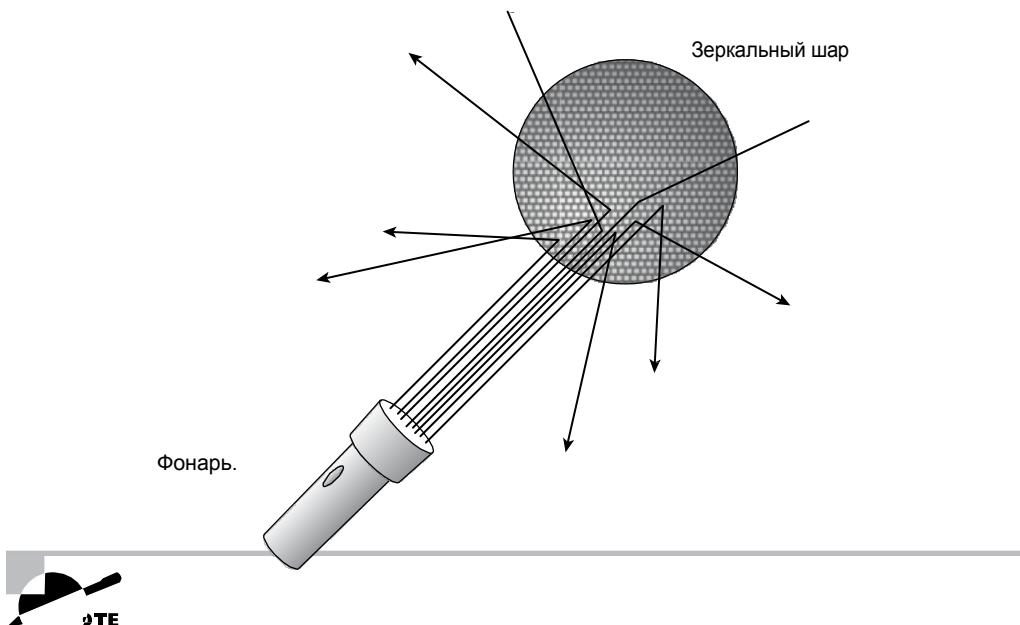
Второй тип рассеивания происходит, когда радиосигнал сталкивается с некоторым типом неровной поверхности и отражается во множество направлений. Заборы из сетки рабицы, проволочная сетка в цементной или гипсовой штукатурках стен, листва деревьев и каменистая местность обычно вызывают такой тип рассеивания. При столкновении с неровной поверхностью, основной сигнал рассеивается на несколько отраженных сигналов, что может привести к существенному ухудшению качества сигнала и может даже привести к потере принимаемого сигнала.

Рисунок 3.13 показывает фонарь, который светит на зеркальный шар для дискотек. Обратите внимание, как основной луч сигнала полностью разбивается на множество отраженных лучей с меньшей амплитудой и во множестве разных направлениях.

## Преломление (рефракция)

В дополнение к тому, что радиосигнал поглощается или отражается (путем отражения или рассеивания), при определенных условиях радиосигнал может действительно отклониться, при поведении известном как *преломление или рефракция [refraction]*. Прямое определение преломления это отклонение радиосигнала при прохождении через среду с различной плотностью, вызывая таким образом изменение направления волны. Радиоволновое преломление наиболее часто происходит в результате атмосферных условий.

**Р И С У Н О К 3.13** Аналогия рассеивания



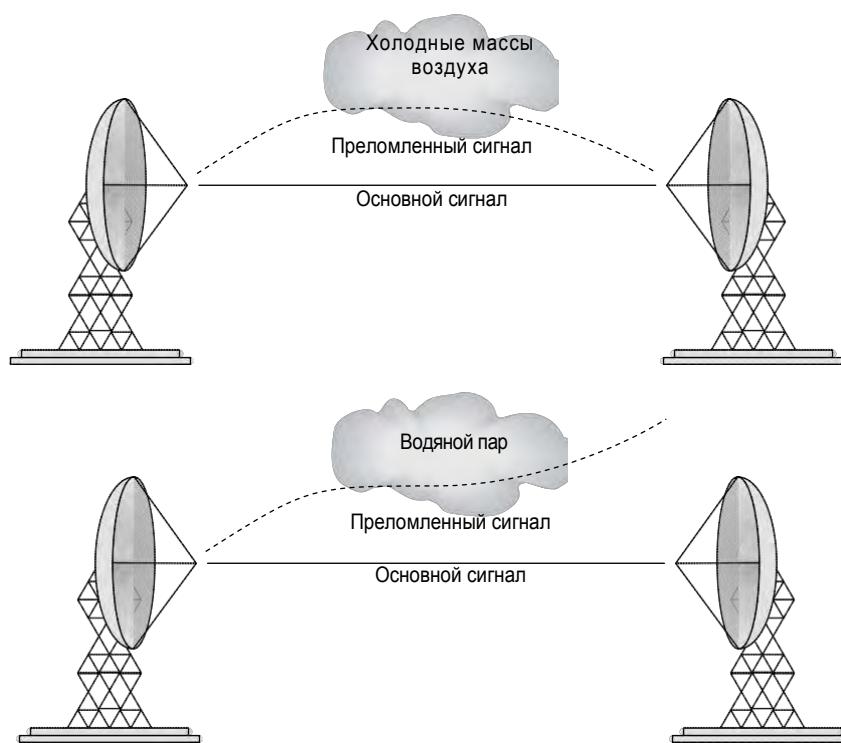
Когда вы имеете дело с каналами связи через внешние мосты с большими пролетами, показатель изменения преломляющей способности, который может стать проблемой, - это то что называется как коэффициент преломления (*k-factor*). Коэффициент *k* равный 1 означает, что нет преломления. Коэффициент *k* меньше 1, например 2/3, означает, что сигнал отклоняется от земли. Коэффициент *k* больше 1 означает отклонение к земле. Нормальные атмосферные условия имеют коэффициент *k* (*k-factor*) равный 4/3, что означает небольшое отклонение в направлении изгиба земли.

Три наиболее общие причины преломления это водяной пар, изменение температуры воздуха, и изменение давления воздуха. Во внешней среде, радиосигналы обычно слегка преломляются по направлению к земной поверхности. Однако, изменения в атмосфере может заставить сигнал отклониться от земли. На каналах связи через длинные внешние беспроводные мосты преломление может быть проблемой. Радиосигнал может также преломляться через определенные виды стекла и другие материалы, которые можно встретить внутри помещений. Рисунок 3.14 показывает два примера преломления.

## Дифракция

Не путать с преломлением (рефракцией), существует еще одно поведение распространения радиоволн, которое также отклоняет радиосигнал, оно называется *дифракцией* [*diffraction*]. Дифракция - это отклонение сигнала вокруг объекта (в то время как Преломление (Рефракция), как вы помните, это отклонение сигнала при прохождении через среду). Дифракция - это отклонение и рассеяние радиосигнала при встрече с препятствием. Условия, которые должны быть соблюдены, чтобы произошла дифракция полностью зависят от формы, размера и материала препятствующего объекта, а также точные характеристики радиосигнала, такие как: поляризация, фаза и амплитуда.

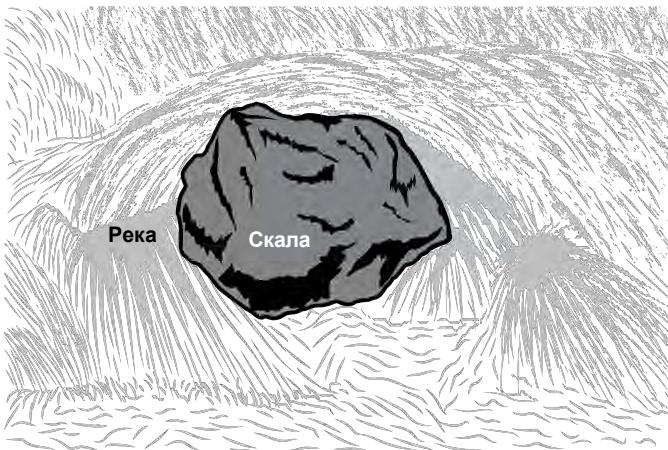
РИСУНОК 3.14 Преломление[Рефракция]



Как правило, дифракция вызвана какой-либо частичной блокировкой радиочастотного сигнала, например, небольшим холмом или зданием, которое находится между передающей радиостанцией и приемником. Волны, которые встречают препятствие огибают объект, проходя более длинный и другой путь. Волны, который не столкнулись с объектом, не отклоняются и сохраняют более короткий и первоначальный путь. Аналогия, изображенная на Рисунке 3.15 – это скала, находящаяся посередине реки. Большая часть течения сохраняет первоначальный поток, однако часть течения, которая сталкивается со скалой, отразится от скалы и еще часть будет огибать скалу (дифрагировать, если можно так сказать).

Находящаяся прямо за препятствием область называется *радиотень* [*RF shadow*]. В зависимости от изменения в направления дифрагированных сигналов, область радиотени может стать мертвым зоной покрытия или по прежнему принимать ухудшенные сигналы. Концепция радиотеней является важной при выборе мест установки антennы. Крепление точки доступа к балке или другой конструкции стены может создать виртуальную слепую радиозону, точно так же, как установка столба создаст тень от установленного на нем источника света..

**РИСУНОК 3.15** Аналогия Дифракции



## Потери (Затухание)

*Потери*[*Loss*], также называется как затухание [*attenuation*], лучше всего описываются как уменьшение амплитуды или силы сигнала. Сигнал может потерять силу при передаче по проводам или по воздуху. На проводной части коммуникаций (РЧ кабель) сигнал электрического переменного тока теряет силу из-за комплексного электрического сопротивления(импеданса) коаксиального кабеля и других компонентов, таких как разъемы (коннекторы).



В Главе 5 мы обсуждаем электрическое комплексное сопротивление (импеданс), которое является мерой сопротивления переменному току. Вы также узнаете о несогласованностях электрического комплексного сопротивления(импеданса), которые могут привести к потере сигнала на проводной части.

После излучения радиосигнала в эфир через antennу, сигнал затухает из-за поглощения, расстояния, или возможно негативных эффектов многолучевого распространения [*multipath*]. Вы уже знаете, что когда радиосигнал проходит через различные среды, в которых сигнал может быть поглощен в среде, что в свою очередь вызывает потерю амплитуды. Разные материалы обычно дают разные результаты затухания. Радиосигнал 2.4 ГГц, который проходит через гипсокартон затухает на 3 децибела (dB), теряя половину начальной амплитуды. Радиосигнал 2.4 ГГц, который поглощается в бетонной стене потеряет 12 dB, т.е. амплитуда уменьшиться в 16 раз от начальной амплитуды. Как обсуждалось ранее, вода – основной источник поглощения, так же как и плотные материалы, такие как шлакоблоки, все приводят к затуханию.

Хотя термин «потеря» может иметь негативный оттенок, затухание не всегда является нежелательным. В Главе 13 вы узнаете, что использование свойств затухания стен для изоляции сигнала может быть действительно полезным. Применение естественных радиочастотных характеристик помещения для получения более хорошего дизайна БЛВС является важной концепцией.

**УПРАЖНЕНИЕ 3.1****Визуальная демонстрация поглощения**

В этом упражнении, используйте веб приложение EMANIM. Перейдите на <https://emanim.szialab.org/index.html> чтобы посмотреть эффекты затухания материалов из-за поглощения.

1. В панели управления справа, щелкните поле выбора, чтобы включить Материал. Длину (Length) материала сделайте 16, коэффициент ослабления (extinction coefficient) для волны 1 сделайте 0.25, а параметр преломления (refraction index) сделайте 1.00.
2. Когда радиоволна пересекает материю, материя поглощает часть волны. В результате, амплитуда волны уменьшается. Коэффициент ослабления определяет какая часть волны поглощается на единицу длины материала.
3. Изменяя длину материала и коэффициент ослабления для Волны 1, посмотрите, как это влияет на поглощение.

И потери, и усиление могут измеряться в относительной мере в изменении мощности, называемой децибелами (dB), которая исчерпывающе обсуждается в Главе 4 «Радио Компоненты, Измерения и Математика». Таблица 3.1 показывает различные значения затуханий для некоторых материалов.

**ТАБЛИЦА 3.1 Сравнение затуханий материалов**

Материал	2.4 ГГц
Лифтовая шахта	-30 dB
Бетонная стена	-12 dB
Деревянная дверь	-3 dB
Нетонированные окна	-3 dB
Гипсокартон	-3 dB
Гипсокартон (пустотелый)	-2 dB
Офисные перегородки рабочих мест	-1 dB



Таблица 3.1 приведена как справочная таблица, а не как информация, которая будет на экзамене CWNA. Действительные измерения могут отличаться от места к месту, в зависимости от конкретных факторов окружающей среды.

Важно понимать, что радиосигнал будет также терять амплитуду даже всего лишь как функция от расстояния из-за потерь в свободном пространстве, которые будут объяснены в следующем разделе. Также свойство отражения при распространении может произвести негативный эффект многолучевого распространения, и в результате, вызвать уменьшение силы сигнала.

## Потери в Свободном Пространстве

По законам физики, электромагнитный сигнал будет затухать по мере движения, несмотря на отсутствие затухания, вызванного препятствиями, поглощением, отражением, дифракцией и так далее. *Потери на Пути в Свободном Пространстве [Free space path loss (FSPL)]* это потеря силы сигнала вызванное естественным расширением волн, часто называемое *расходностью (дивергенцией) луча [beam divergence]*. Энергия радиосигнала распределяется по большей площади по мере удаления сигнала от антенны, и в результате, сила сигнала уменьшается.

Один способ проиллюстрировать потери в свободном пространстве — это использовать аналогию с воздушным шаром. До того, как воздушный шар наполнен воздухом, он остается маленьким, но с толстой плотной резиной. После того, как воздушный шар надулся и увеличился в размерах, резина становится очень тонкой. Радиосигнал теряет силу точно таким же способом. К счастью, эти потери в силе сигнала являются логарифмическими, а не линейными; таким образом, амплитуда не уменьшается так же сильно на втором отрезке одинаковой длины, как она уменьшается на первом отрезке. В зависимости от центральной частоты отдельного канала, сигнал на 2.4ГГц уменьшиться на 80 дБ через 100 метров. Через те же 100 метров сигнал 5ГГц потеряет около 87 дБ, а потеря мощности 6ГГц сигнала будет около 89 дБ. Сигналы всех трех частот потеряют еще только 6дБ на следующих 100 метрах.

Вот формулы для вычисления затухания на пути в свободном пространстве:

$$\text{FSPL} = 36.6 + 20 \log_{10} (f) + 20 \log_{10} (D)$$

FSPL = потери в свободном пространстве в дБ

f = частота в МГц

D = расстояние в милях между антеннами

$$\text{FSPL} = 32.44 + 20 \log_{10} (f) + 20 \log_{10} (D)$$

FSPL = потери в свободном пространстве в дБ

f = частота в МГц

D = расстояние в километрах между антеннами



Формулы потерь в свободном пространстве приведены в качестве справочного материала и не включены в экзамен CWNA. Множество онлайн калькуляторов FSPL и других калькуляторов для радиопараметров можно найти в Интернете простым поиском.

Еще более простой способ оценить потери в свободном пространстве (FSPL) называется *правило 6 дБ*. (Вспомните, что децибелы это мера усиления или затухания(потерь); более детально о дБ исчерпывающе раскрыто в Главе 4) Правило 6 дБ гласит, что удваивание расстояния дает уменьшение амплитуды на 6 дБ, независимо от частоты. Таблица 3.2 показывает оценочные потери в свободном пространстве и подтверждает правило 6 дБ.

**ТАБЛИЦА 3.2** Затухания из за потерь в свободном пространстве

Расстояние (метры)	Затухание (дБ)		
	2.437 ГГц (Канал 6 в полосе 2.4 ГГц )	5.500 ГГц (Канал 100 в полосе 5 ГГц)	6.675 ГГц (Канал 145 в полосе 6 ГГц)
1	40.18	47.25	48.93
10	60.18	67.25	68.93
100	80.18	87.25	88.93
1000	100.20	107.20	108.9
2000	106.20	113.30	114.90
4000	112.20	119.30	121.00
8000	118.20	125.30	127.00



### Пример из Реальной Жизни

#### Почему Потери в Свободном Пространстве Так Важны?

Все радио устройства имеют, что называется *приемный уровень чувствительности*. Радиоприемник может правильно интерпретировать и принять сигнал до конкретного нижнего фиксированного порога амплитуды. Если радиомодуль принимает сигнал выше этого амплитудного порога, то сигнал достаточно мощный для того чтобы радиомодуль обнаружил и интерпретировал сигнал. Например, если вы шептали кому-то секрет, вам нужно было быть уверенным, что ваш шепот достаточно громок чтобы тот, кому вы шепчете, мог услышать и понять его.

Если амплитуда принимаемого сигнала ниже порога чувствительности приема радиомодуля, радиомодуль больше не может правильно воспринимать и интерпретировать сигнал. Концепция потерь в свободном пространстве также применима к дорожным путешествиям на вашем автомобиле. Когда вы в автомобиле слушаете АМ радиостанцию, в конце концов вы выезжаете за пределы диапазона и радиоприемник больше не способен принимать и обрабатывать музыку.

В дополнение к тому, чтобы радиомодуль был способен принимать и интерпретировать сигнал, принимаемый сигнал должен быть не только достаточно сильным, чтобы его

можно было услышать, но и достаточно сильным, чтобы его можно было услышать выше любого фонового радиошума, обычно называемого *уровнем фонового радиошума [noise floor]*. Сигнал должен быть громче, чем любой фоновый шум. В примере нашептывания секрета кому-то, если бы вы сообщали шепотом секрет во время проезда скорой помощи с включенной сиреной, даже если бы ваш шепот был бы достаточно громким чтобы его можно было слышать, шум от сирены был бы слишком громким для человека чтобы различить что вы говорите.

При проектировании и внутренних БЛВС, и внешних каналов связи через беспроводные мосты, вы должны быть уверенными, что радиосигнал не уменьшиться ниже приемного уровня чувствительности вашего радиомодуля БЛВС просто из-за потерь в свободном пространстве, и вы должны убедится что сигнал не уменьшиться до или ниже уровня фонового радиошума. Обычно эта цель для помещений достигается путем проведения радиообследования или обследования места[site survey]. Каналы связи по внешним мостам требуют серии вычислений, называемых *бюджетом линии [link budget]*. (Радиообследование описано в Главе 14, “Обследование места и Контрольная проверка,” а бюджеты линии описаны в Главе 4.)

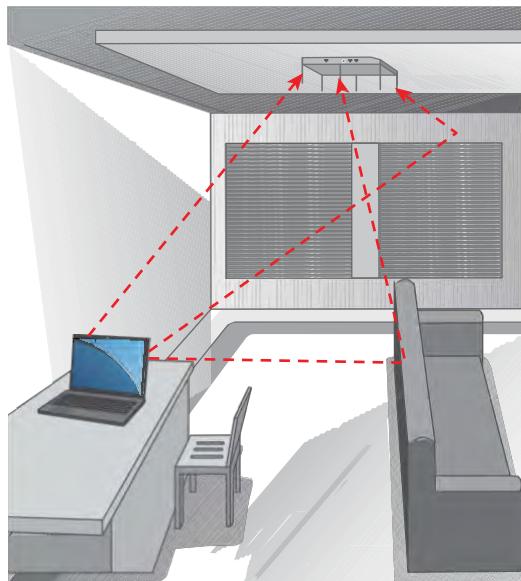
## Многолучевое распространение

*Многолучевое распространение [Multipath]* это явление распространения, которое является результатом двух и более путей, по которым сигнал прибывает на приемную антенну в тоже самое время или в пределах наносекунд друг от друга. Из-за естественного расширения волн поведение распространения во время отражения, рассеяния, дифракции и преломления будет происходить по-разному в разных средах.. Когда сигнал встречается с объектом, он может отразиться, рассеяться, преломиться или дифрагировать. Все эти особенности поведения могут привести к многолучевому распространению одного и того же сигнала.

В помещении отраженные сигналы и эхо могут быть вызваны длинными коридорами, стенами, столами, полами, шкафами с папками и многими другими препятствиями. Помещения с большим количеством металлических поверхностей, такие как ангары самолетов, склады и фабрики, печально известны своим многолучевым распространением из-за всех отражающих поверхностей. Отражение обычно является основной причиной образования сред с высокой степенью многолучевого распространения.

На открытом воздухе многолучевое распространение может быть вызвано ровной дорогой, большим водоемом, зданием или атмосферными условиями. Поэтому у нас есть сигналы, отражающиеся и изгибающиеся в разных направлениях. Основной сигнал по-прежнему будет проходить к приемной антенне, но некоторые отраженные и отклоненные сигналы также могут попасть к приемной антенне по другим путям. Другими словами, множество путей радиосигнала приходят на приемник, как показано на Рисунке 3.16.

**РИСУНОК 3.16** Многолучевое распространение



Обычно отраженным сигналам требуется немного больше времени, чтобы достичь приемной антенны, потому что они должны пройти большее расстояние, чем основной сигнал. Разница во времени между этими сигналами может измеряться миллиардными долями секунды (наносекундами). Разница во времени между этими всеми путями называется как *разброс по времени задержки [delay spread]*. Далее в этой книге вы узнаете, что некоторые технологии расширения спектра более терпимы, чем другие, когда они сталкиваются с разбросом по задержке.

Итак, что именно происходит, когда собственно присутствует многолучевое распространение? Во времена передачи устаревшего аналогового телевизионного сигнала многолучевое распространение вызывало видимый призрачный эффект с блеклым дубликатом справа от основного изображения. При передаче современного цифрового телевидения многолучевое распространение может проявляться в виде пикселизации, зависаний или, в худшем случае, полной потери изображения из-за повреждения данных. С радиосигналами эффекты многолучевого распространения могут быть как конструктивными, так и деструктивными. Из-за разницы в фазе этих многих путей, суммарный сигнал часто будет уменьшаться, усиливаться и становиться поврежденным. Эти эффекты иногда называются *Рэлеевским замиранием [Rayleigh fading]*, еще одно явление, названное в честь Британского физика Лорда Рэлея.

Четыре возможных результата многолучевого распространения:

**Усиливающее Замирание [Upfade]** Это увеличенная сила сигнала. Когда множество путей радиосигнала прибывают на приемник в тоже самое время и в фазе или частично не в фазе с основной волной, результатом является увеличение силы сигнала (амплитуды). Небольшая разность фаз от 0 до 120 градусов будет вызывать *усиливающее замирание [upfade]*. Однако, поймите, пожалуйста, что окончательный принятый сигнал никогда не сможет быть сильнее исходного переданного сигнала из-за потерь в свободном пространстве. Усиливающее замирание является примером конструктивного многолучевого распространения.

**Уменьшающее Замирание[Downfade]** Это уменьшенная сила сигнала. Когда множество путей радиосигнала прибывают на приемник в тоже самое время, но не в фазе с основной волной, результатом является уменьшение силы сигнала (амплитуды). Разность фаз в диапазоне между 121 и 179 градусами будет вызывать *уменьшающее замирание [downfade]*. Уменьшенная амплитуда в результате многолучевого распространения считается деструктивным многолучевым распространением.

**Обнуление [Nulling]** Это погашение сигнала. Когда множество путей радиосигнала прибывают на приемник в тоже самое время и с разницей 180 градусов по фазе с основной волной, результатом будет *обнуление [nulling]*. Обнуление это полное исчезновение радиосигнала. Полное исчезновение сигнала является очевидно деструктивным.

**Повреждение данных [Data Corruption]** Из-за разницы во времени между основным сигналом и отраженными сигналами (называемой как разброс по времени задержки), вместе с тем фактом, что может быть много отраженных сигналов, приемник может иметь проблемы во время демодуляции информации радиосигнала. Разница во времени в задержках может привести к наложению битов друг на друга, и в итоге - повреждение данных. Этот тип многолучевой интерференции часто называют *межсимвольной интерференцией [intersymbol interference (ISI)]*. Повреждение данных является наиболее частым случаем деструктивного многолучевого распространения.

Плохая новость в том, что среди с высоким уровнем многолучевого распространения могут привести к повреждению данных из-за межсимвольной интерференции вызванной разным временем задержек. Хорошая новость в том, что принимающая станция обнаружит ошибки с помощью определенной в 802.11 циклическим избыточным кодом (CRC), так как контрольная сумма не будет рассчитана точно. Стандарт 802.11 требует, чтобы большинство однократных (unicast) кадров были подтверждены

принимающей станцией кадром подтверждения (ACK); в противном случае передающей станции придется повторить передачу кадра. Приемник не подтвердит кадр, который не прошел проверку CRC. Поэтому, к сожалению, кадр должен быть передан повторно, но это лучше, чем он будет неправильно интерпретирован.

Повторные передачи Уровня 2 негативно влияют на общую пропускную способность любой БЛВС 802.11, а также могут повлиять на доставку чувствительных ко времени пакетов приложений, таких как VoIP. В главе 15, “Решение проблем БЛВС,” мы обсуждаем множество причин повторных передач уровня 2, как их решать и минимизировать. Многолучевое распространение является одной из главных причин повторных передач уровня 2, которые негативно влияют на пропускную способность и задержку устаревшей беспроводной связи 802.11a/b/g. На радиопередачах 802.11n/ac/ax, которые используют антеннное разнесение много-вводов, много-выходов (MIMO) и технику обработки сигналов *комбинация максимальных отношений [maximal ratio combining (MRC)]*, многолучевое распространение имеет конструктивный эффект.

В прошлом необходимо было бороться с повреждением данных при передаче устаревших 802.11a/b/g, вызванным многолучевым распространением, а использование однонаправленных антенн для уменьшения отражений было обычным явлением в помещениях с высоким уровнем многолучевого распространения. С технологией MIMO, используемой радиомодулями 802.11n/ac/ax, многолучевое распространение теперь наш друг, и однонаправленные антенны теперь редко нужны в помещениях. Однако, однонаправленные MIMO панельные антенны могут все еще использоваться внутри помещений, чтобы обеспечить секторное покрытие в среде с высокой плотностью пользователей.

**У П Р А Ж Н Е Н И Е 3 . 2****Визуальная Демонстрация Многолучевого распространения и Фазы**

В этом упражнении, вам нужно использовать веб приложении EMANIM. Перейдите на <https://emanim.szialab.org/index.html> чтобы просмотреть эффект затухания материалов из-за поглощения. В этом упражнении вы увидите влияние на амплитуду различных фаз двух сигналов, поступающих одновременно.

1. Сбросьте настройки от предыдущей лабораторной работы к настройкам по умолчанию.
2. В контрольной панели справа, щелкните поле выбора , чтобы включить Волну 1(Wave 1) и Волну 2 (Wave 2).
3. Обе волны должны быть установлены в Вертикальную Поляризацию (Vertical Polarization) с Амплитудой (Amplitude) 5 и Длиной волны (Wavelength) 5. Поле выбора «Волна 1 + Волна 2»(“Wave 1 + Wave 2”) должно быть отмечено, поле Обратное Направление (Reverse Direction) должно быть не отмечено, а Разница Фаз (Phase Difference) должна быть 0.

Две идентичные, вертикально поляризованные волны накладываются друг на друга. (Вы не можете видеть обе сразу, потому что они накрывают друг друга). Синяя волна представляет собой объединенную амплитуду обеих волн.

4. Теперь измените разность фаз на **-70**.

Две идентичные, с 70 градусной разницей по фазе волны накладываются друг на друга. Результатом является волна со слегка увеличенной амплитудой по сравнению с составляющими волнами.

5. Измените снова разность фаз, в этот раз на **-140**.

Две идентичные, с 140 градусной разницей по фазе волны накладываются друг на друга. Результатом является волна с уменьшенной амплитудой по сравнению с

6. Наконец, измените разность фаз на **-180**.

Две идентичные, вертикально поляризованные волны накладываются друг на друга. Результатом является погашение двух волн.

---

## Усиление

*Усиление [Gain(Amplification)]*, можно лучше всего описать как увеличение амплитуды или силы сигнала. Известно два типа усиления: активное усиление и пассивное усиление. Амплитуда сигнала может быть увеличена за счет использования внешних устройств.

*Активное усиление [Active gain]* обычно обусловлено приемопередатчиком (трансивером) или использованием усилителя на проводе, который соединяет приемопередатчик с антенной. Большинство Wi-Fi трансиверов способны передавать на разных уровнях мощности, создавая более высокими уровнями мощности более сильный сигнал. Усилитель обычно двунаправленный, что означает что он увеличивает и входящее и исходящее напряжение переменного тока. Устройства активного усиления требуют использовать внешний источник энергии.

*Пассивное усиление [Passive gain]* достигается за счет фокусировки радиосигнала с использованием антенны. Антенны – это пассивные устройства, которые не требуют внешний источник энергии. Вместо этого внутренняя работа антенны сильнее фокусирует сигнал в одном направлении, чем в другом. Увеличение амплитуды сигнала является результатом либо активного усиления до того, как сигнал достигает антенны, либо пассивного усиления, фокусирующего сигнал, излучаемый антенной.

---

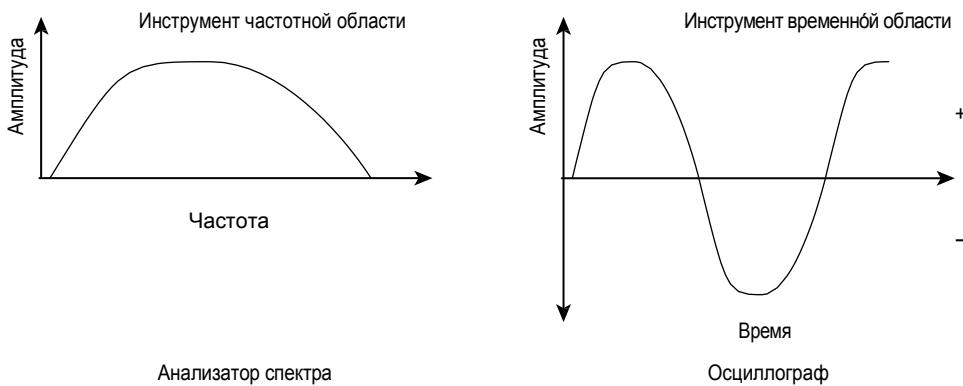


Правильное использование антенн подробно описано в Главе 5.

## Инструменты радиоанализа

Два совершенно разных инструмента радиоанализа может быть использовано, чтобы представить радиосигнал. Оба инструмента могут показывать измерение амплитуды радиосигнала в заданной точке. Первый - это инструмент частотной области, который может быть использован для измерения амплитуды на ограниченном частотном спектре. Частотный инструмент, используемый БЛВС инженерами, называется *анализатор спектра [spectrum analyzer]*. Второй инструмент, инструмент временной области, может быть использован для измерения того как изменяется амплитуда сигнала с течением времени. Общепринятое название для инструмента временной области - *осциллограф [oscilloscope]*. Рисунок 3.17 показывает как оба эти инструмента могут быть использованы для отображения амплитуды. Следует заметить, что анализатор спектра часто используется инженерами БЛВС во время радиообследования. Осциллограф используется редко, если вообще используется, при развертывании Wi-Fi сети; однако, осциллографы используются радиоинженерами в лабораторных тестовых средах. Веб приложение EMANIM, упоминаемое ранее в этой главе, является эффективным симулятором временной области.

**Р И С У Н О К 3.17** Инструменты анализа радиосигнала



# Итого

В этой главе была рассмотрена сама суть, основы радиосигналов. Чтобы правильно проектировать и администрировать беспроводные сети, важно иметь четкое понимание следующих принципов свойств и особенностей поведения радиосигналов:

- Электромагнитные волны и как они создаются
- Отношение между длиной волны, частотой и скоростью света
- Сила сигнала и различные пути, в которых сигнал может ослабиться или усилиться
- Важное значение отношения между двумя и более сигналами
- Как двигается сигнал отклоняясь, отражаясь или поглощаясь каким-либо образом

Когда вы ищите проблему на сети Ethernet, лучшее место для старта - это всегда уровень 1, Физический уровень. Поиск и устранение проблем на Wi-Fi также должен начинаться с Физического уровня. Изучение основ радиотехники, которые присутствуют на уровне 1 является значимым шагом в правильном администрировании беспроводной сети.

## Темы Экзамена

**Понимание длины волны, частоты, амплитуды и фазы.** Знать определение каждой радиоволновой характеристики и как каждая может повлиять на дизайн БЛВС

**Помнить все виды распространения радиоволн.** Быть способным объяснить разницу между разными видами распространения волн (такими, как отражение, дифракция, рассеяние и т.д.) и различные среды, которые ассоциируются с каждым видом распространения.

**Понимание причин затухания.** Затухание (потери) может происходить и на проводе и в эфире. Поглощение, потери в свободном пространстве, многолучевое ослабляющее замирание - все вызывают затухание.

**Определение потерь в свободном пространстве.** Несмотря на отсутствие каких-либо препятствий, электромагнитные волны затухают логарифмически по мере удаления от передатчика.

**Помнить четыре возможных результата многолучевого распространения и его связь с фазой.** Многолучевое распространение может стать причиной ослабляющего замирания, усиливающего замирания, обнуления и повреждения данных. Понимать, что эффекты многолучевого распространения могут быть как деструктивным так и конструктивным.

**Знать результаты межсимвольной интерференции и разброса задержки по времени.** Разница по времени между основным сигналом и отраженными сигналами может вызвать повреждение битов и повлиять на пропускную способность и задержку из-за повторных передач на 2 уровне.

**Объяснить разницу между активным и пассивным усилением.** Приемопередатчики (Трансиверы) и усилители радиосигнала являются активными устройствами, в то время как антенны являются пассивными устройствами.

**Объяснить разницу между амплитудой на передаче и на приеме.** Амплитуда передачи обычно определяется как размер начальной амплитуды, которая покидает радиопередатчик. Когда радиомодуль принимает радиосигнал, сила принимаемого сигнала наиболее часто называется амплитуда на приеме.

## Контрольные Вопросы

1. Каковы результаты интерференции многолучевого распространения? (Выберите все, что применимо.)
  - A. Задержка рассеивания [Scattering delay]
  - B. Усиливающее замирание [Upfade]
  - C. Чрезмерные повторные передачи [Excessive retransmissions]
  - D. Поглощение [Absorption]
2. Какой термин лучше всего определяет линейное расстояние, пройденное за одно колебание положительное-отрицательное-положительное электромагнитного сигнала?
  - A. Гребень [Crest]
  - B. Частота [Frequency]
  - C. Впадина [Trough]
  - D. Длина волны [Wavelength]
3. Какое из следующих утверждений об усилении является верным? (Выберите все, что применимо.)
  - A. Антенны являются усилителями с активным усилением, которые фокусируют энергию сигнала.
  - B. Приемопередатчики(Трансиверы) являются усилителями с активным усилением, откуда поступает сигнал.
  - C. Антенны являются усилителями с пассивным усилением, которые фокусируют энергию сигнала.
  - D. Радиочастотные усилители пассивно увеличивают силу сигнала фокусируя переменный ток сигнала.
4. Как называется стандартная мера частоты?
  - A. Герц
  - B. Миливatt
  - C. Наносекунда
  - D. Децибел
  - E. K-фактор (K-factor)
5. Когда радиосигнал изгибаются вокруг объекта, этот вид распространения называется как ?
  - A. Расслоение [Stratification]
  - B. Преломление [Refraction]
  - C. Рассеяние [Scattering]
  - D. Дифракция [Diffraction]
  - E. Затухание [Attenuation]
6. Когда множество радиосигналов прибывает на приемник в одно и то же время и генерированы одним и тем же передатчиком, что из следующего может быть результатом комбинированной(суммарной) фазы сигнала?

- A.** 140 градусов расхождения по фазе, усиление  
**B.** 140 градусов расхождения по фазе, погашение  
**C.** 0 градусов расхождения по фазе, усиление  
**D.** 180 градусов расхождения по фазе, ослабление  
**E.** 180 градусов расхождения по фазе, усиление  
**F.** 180 градусов расхождения по фазе, погашение
- 7.** Какое из следующих утверждений является верным? (Выберите все, что подходит.)
- A.** Когда происходит усиливающее замирание [upfade], итоговый сигнал будет сильнее, чем исходный переданный сигнал.  
**B.** Когда происходит уменьшающее замирание [downfade], итоговый принятый сигнал никогда не будет сильнее исходного переданного сигнала.  
**C.** Когда происходит усиливающее замирание [upfade], итоговый полученный сигнал никогда не будет сильнее, чем исходный переданный сигнал.  
**D.** Когда происходит уменьшающее замирание [downfade], итоговый принятый сигнал будет сильнее, чем исходный переданный сигнал.
- 8.** Какая частота радиосигнала, который выполняет 2,4 миллиона циклов в секунду?
- A.** 2.4 герца  
**B.** 2.4 МГц  
**C.** 2.4 ГГц  
**D.** 2.4 килогерца  
**E.** 2.4 КГц
- 9.** Что является лучшим примером инструмента временной области, который может быть использован радиоинженером?
- A.** Осциллограф [Oscilloscope]  
**B.** Спектроскоп [Spectroscope]  
**C.** Анализатор спектра [Spectrum analyzer]  
**D.** Рефракционный гастроскоп [Refractivity gastroscope]
- 10.** Какие объекты или материалы в основном вызывают отражение? (Выберите все, что подходит.)
- A.** Металл  
**B.** Деревья  
**C.** Асфальтовая дорога  
**D.** Озеро  
**E.** Полы с ковровым покрытием
- 11.** Какой из этих видов распространения может привести к многолучевому распространению? (Выберите все, что подходит.)
- A.** Преломление [Refraction]  
**B.** Дифракция [Diffraction]  
**C.** Усиление [Amplification]  
**D.** Рассеяние [Scattering]

- E.** Затухание [Attenuation]
  - F.** Отражение [Reflection]
- 12.** Какое поведение можно описать как: радиосигнал сталкивается с забором из сетки, в результате чего сигнал отскакивает в нескольких направлениях?
- A.** Дифракция [Diffraction]
  - B.** Рассеяние [Scattering]
  - C.** Отражение [Reflection]
  - D.** Преломление [Refraction]
  - E.** Мультиплексирование [Multiplexing]
- 13.** Какие радио технологии стандарта 802.11 наиболее подвержены деструктивному влиянию многолучевого распространения? (Выберите все, что подходит.)
- A.** 802.11a
  - B.** 802.11b
  - C.** 802.11g
  - D.** 802.11n
  - E.** 802.11ac
  - F.** 802.11ax
- 14.** Что из следующего может вызвать преломление(рефракцию) радиосигнала при прохождении через него? (Выберите все, что подходит.)
- A.** Перепад температуры воздуха
  - B.** Изменение давления воздуха
  - C.** Влажность
  - D.** Гроза
  - E.** Ветер
  - F.** Смог
- 15.** Какое из следующих выражений о потерях в свободном пространстве являются верными? (Выберите все, что подходит.)
- A.** Радиосигналы затухают по мере распространения, несмотря на отсутствие затухания вызванного препятствиями.
  - B.** Пространственные потери происходят с постоянной линейной скоростью.
  - C.** Затухание вызвано только препятствиями
  - D.** Пространственные потери происходят с логарифмической скоростью.
- 16.** Какой термин используется, чтобы описать разницу по времени между основным сигналом и отраженным сигналом приходящими на приемник?
- A.** Задержка распространения
  - B.** Расширение спектра

- C.** Многолучевое распространение  
**D.** Разброс задержки
- 17.** Что является примером инструмента частотной области, который может быть использован радиоинженером?
- A.** Осциллограф [Oscilloscope]  
**B.** Спектроскоп [Spectroscope]  
**C.** Анализатор спектра [Spectrum analyzer]  
**D.** Рефракционный гастроскоп [Refractivity gastroscope]
- 18.** Применяя знания о свойствах радиоволн и видах их поведения, какие две опции должны больше всего волновать инженера БЛВС при проведении радиоисследования помещения?  
(Выберите два наиболее подходящих ответа.)
- A.** Бетонные стены  
**B.** Температура помещения  
**C.** Заштукатуренные стены из деревянных реек.  
**D.** Гипсокартон
- 19.** Какие три свойства являются взаимосвязанными?
- A.** Частота, длина волны, и скорость света  
**B.** Частота, амплитуда, и скорость света  
**C.** Частота, фаза, и амплитуда  
**D.** Амплитуда, фаза, и скорость звука
- 20.** Какое вид распространения радиосигнала лучше всего описывает сигнал, сталкивающийся со средой и отклоняющийся в разных направлениях?
- A.** Преломление(Рефракция) [Refraction]  
**B.** Рассеяние [Scattering]  
**C.** Диффузия [Diffusion]  
**D.** Дифракция [Diffraction]  
**E.** Микроволновое отражение [Microwave reflection]



# Глава **4**



# Компоненты, Параметры, и Математика Радиосвязи

---

**В ЭТОЙ ГЛАВЕ, ВЫ УЗНАЕТЕ О СЛЕДУЮЩЕМ:**

✓ **Компоненты радиосвязи**

- Передатчик
- Антenna
- Приемник
- Расчетный излучатель
- Эквивалентная Изотропно Излучаемая Мощность (ЭИИМ (EIRP))

✓ **Единицы мощности и сравнения**

- Ватт (Вт)
- Милливатт (мВт)
- Децибел (дБ)
- Децибели относительно изотропного излучателя (дБи)
- Децибели относительно полуволновой дипольной антенны (дБд)
- Децибели относительно 1 милливатта (дБм)
- Закон обратного квадрата

✓ **Радиоволновая математика**

- Правило 10 (десяток) и 3 (троек)



- ✓ **Уровень Фонового шума**
- ✓ **Отношение Сигнал-Шум (SNR)**
  - Отношение Сигнал к Интерференция плюс Шум (SINR)
- ✓ **Индикатор Силы Принимаемого Сигнала (RSSI)**
- ✓ **Бюджет Линии Связи**
  - Запас на замирания/рабочий запас системы



Проще говоря, передача данных — это передача информации между компьютерами. Независимо от того, какая форма связи используется, для успешной передачи требуется множество компонентов.

Прежде чем рассматривать отдельные компоненты, давайте сначала упростим ситуацию и рассмотрим три основных требования для успешной коммуникации (связи):

- Два или более устройств, которые хотят обмениваться данным.
- Должна быть среда, средство или метод, которые они могли бы использовать для связи.
- Должен быть набор правил для них, чтобы использовать их при общении. (Это описано в Главе 8, “802.11 Доступ к Среде.”)

Эти три основных требования одинаковы для всех форм связи, будь то беседа группы людей за званым обедом или множество компьютеров, обменивающихся данными через беспроводную сеть.

Существование компьютерной сети фактически подразумевает, что первое требование выполнено. Если бы у нас не было двух или более устройств, которые хотели бы обмениваться данными, нам вообще не нужно было бы создавать сеть. Сертификация CWNA это также подразумевает, и поэтому, редко, если вообще когда-либо, заботится специально о, собственно, самих данных. Предполагается, что у нас есть данные; наша забота состоит в том, чтобы передать и получить их.

Эта глава фокусируется на втором требовании: среда, средства или методы связи. Мы раскроем компоненты радиосвязи, которые составляют то, что мы называем среда беспроводной передачи. Здесь мы коснемся передачи радиосигнала и роли каждого устройства и компоненты на всем пути передачи. Мы также покажем, как каждое устройство или компонента влияют на передачу.

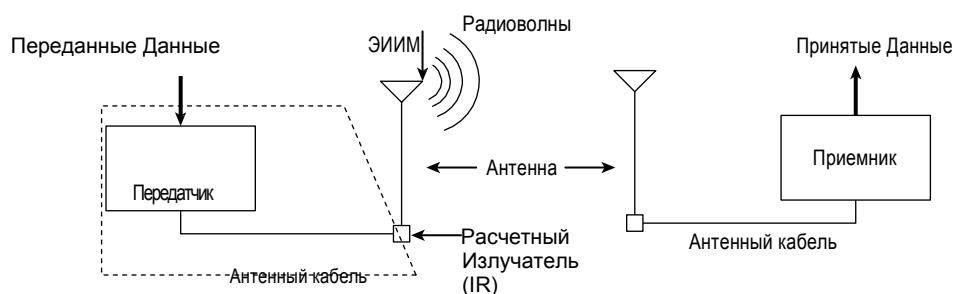
В Главе 3, “Основы Радиотехники,” вы узнали, что существует много видов поведения радиоволн, которые влияют на сигнал, как только он покинул передатчик и отправился к приемнику. По мере движения сигнала через различные компоненты радиосистемы, и затем распространяясь через воздух (эфир), амплитуда сигнала изменяется. Некоторые компоненты увеличивают мощность сигнала (усиление), в то время как другие компоненты уменьшают мощность (затухание или потери). В этой главе вы узнаете, как количественно определить и измерить мощность волн, а также рассчитать, как на волны влияют как внутренние, так и внешние воздействия. Используя эти вычисления, вы сможете определить, будут ли у вас средства для связи между устройствами.

# Компоненты радиосвязи

Многие компоненты способствуют успешной передаче и приему радиосигнала. Рисунок 4.1 показывает ключевые компоненты, которые описаны в следующих разделах. В дополнение к знанию функций компонентов важно понимать, как каждый из компонентов конкретно влияет на силу сигнала.

РИСУНОК 4.1

Радио компоненты



Позже в этой главе, когда мы будем обсуждать радио математику, вы увидите, как вычислить эффект, который имеет каждый компонент на сигнал.

## Передатчик

*Передатчик [transmitter]* является начальным компонентом в создании беспроводной среды. Компьютер передает данные передатчику, и задача передатчика — начать радиосвязь.

В Главе 1, “Обзор Беспроводных Стандартов, Организаций и Основы,” вы узнали о несущих сигналах и методах модуляции. Когда передатчик получает данные, он начинает генерировать сигнал переменного тока. Этот сигнал переменного тока определяет частоту. Например, для сигнала 2,4 ГГц, сигнал переменного тока колеблется около 2,4 миллиарда раз в секунду, тогда как для сигнала 5 ГГц, сигнал переменного тока колеблется около 5 миллиардов раз в секунду. Это колебание определяет частоту радиоволны.



Точные используемые частоты описаны в Главе 6, “Беспроводные Сети и Технологии Расширения Спектра.”

Передатчик принимает предоставленные данные и модифицирует сигнал переменного тока, используя технику модуляции чтобы закодировать данные в сигнал. Этот модулированный сигнал переменного тока является теперь несущим сигналом, содержащем (или несущим) данные подлежащие передаче. Затем несущий сигнал передается либо прямо на антенну, либо по кабелю к антенне.

В дополнение к генерации сигнала на определенной частоте передатчик отвечает за определение исходной амплитуды передачи или того, что чаще называют *уровнем мощности [power level]*, передатчика. Чем выше амплитуда волны, тем мощнее волна и тем дальше она может быть принята. Уровни мощности, которые разрешено генерировать передатчику, определяются местными регулирующими органами, такими как Федеральная комиссия по связи (FCC) в Соединенных Штатах, и Государственная Комиссия по Радиочастотам (ГКРЧ) в России.



Хотя в этой главе мы объясняем передатчик и приемник отдельно, и хотя функционально они являются разными компонентами, на самом деле они представляют собой одно устройство, которое называется *приемопередатчиком (трансивером [transceiver])* (передатчиком/приемником). Типичными беспроводными устройствами со встроенными приемопередатчиками являются точки доступа, мосты и клиентские адAPTERы.

## Антенна

Антенна выполняет две функции в системе связи. При подключении к передатчику она собирает сигнал переменного тока, который она получает от передатчика, и направляет или излучает радиоволны в сторону от антенны в форме характерной для типа антенны. При подключении к приемнику антенна принимает радиоволны, которые она получает по воздуху, и направляет сигнал переменного тока на приемник. Приемник преобразует сигнал переменного тока в биты и байты. Как вы увидите далее в этой главе, принимаемый сигнал намного слабее генерируемого. Эта потеря сигнала аналогична ситуации, когда два человека пытаются поговорить друг с другом с противоположных концов футбольного поля. Только из-за расстояния (свободного пространства) крик с одного конца поля может быть слышен чуть громче, чем шепот на другом конце.

Радиопередачу антенны обычно сравнивают или соотносят с изотропным излучателем. *Изотропный излучатель [isotropic radiator]* - это точечный источник *[point source]*, который излучает сигнал одинаково во всех направлениях. Солнце - вероятно один из лучших примеров изотропного излучателя. Оно генерирует одинаковое количество энергии во всех направлениях. К сожалению, невозможно изготовить антенну, которая является идеальным изотропным излучателем. Структура самой антенны влияет на выход антенны, подобно тому, как структура колбы лампочки влияет на ее способность излучать свет одинаково во всех направлениях.

Есть два способа увеличить выходную мощность антенны. Первый, это генерировать больше мощности на передатчике, как сказано в предыдущем разделе. Другой, это направить, или сфокусировать радиосигнал, который излучается от антенны. Это похоже на то, как вы можете сфокусировать свет от фонарика. Если снять линзу с фонарика, лампа обычно не очень яркая и излучает практически во всех направлениях. Чтобы сделать свет ярче, вы можете использовать более мощные батареи или снова надеть линзу. Линзы на самом деле не создают больше света, они всего лишь фокусируют свет, который был излучен во всех различных направлениях в узкую область. Некоторые антенны излучают волны, подобно тому, как это делает лампа без линзы, в то время как другие излучают сфокусированные волны, подобные тому, как это делает фонарик с линзой.



В Главе 5, “Радиосигнал и Концепция Антенн,” вы узнаете о типах антенн и как правильно и наиболее эффективно использовать их.

## Приемник

*Приемник [receiver]* является последним компонентом беспроводной среды. Приемник принимает несущий сигнал, полученный от антенны, и переводит модулированные сигналы в 1 (единицы) и 0 (нули). Затем он берет эти данные и передает их на компьютер для обработки. Работа приемника не всегда проста. Полученный сигнал является гораздо менее мощным сигналом, чем тот, который был передан, из-за расстояния, которое он прошел, и эффектов потерь в свободном пространстве (FSPL). Сигнал также часто неспециально изменяется из-за помех от других радиоисточников и многолучевого распространения.

## Расчетный Излучатель

Часть 15 Свода федеральных правил (CFR) FCC определяет *Расчетный излучатель [Intentional Radiator(IR)]* как «устройство, которое специально генерирует и излучает радиоволновую энергию путем излучения или индукции». По сути, это то, что специально разработано для генерации радиоволн, в отличие от того, что генерирует радиоволны как побочный продукт своей основной функции, например, двигатель, который случайно генерирует радиошум.

Регулирующие органы, такие как FCC, ограничивают количество энергии, которое разрешено генерировать расчетному излучателю (IR). Расчетный излучатель (IR) состоит из всех компонентов от передатчика до антенны, но не включая антенну, как показано на Рисунке 4.1. Таким образом, выходная мощность расчетного излучателя (IR) представляет собой сумму всех компонентов от передатчика до антенны (опять же, не включая антенну). Компоненты, составляющие Расчетный излучатель (IR), включают передатчик, все кабели и разъемы, а также любое другое оборудование (заземляющие разъемы, грозовые разрядники, усилители, аттенюаторы и т. д.) между передатчиком и антенной. Мощность расчетного излучателя измеряется на разъеме, который является входом для антенны. Поскольку это точка, в которой измеряется и регулируется Расчетный излучатель (IR), мы часто называем только эту точку Расчетный излучатель (IR). Этот уровень мощности обычно измеряется в милливаттах (мВт) или децибелах относительно 1 милливатт (дБм). Используя аналогию фонарика, Расчетный излучатель - это все компоненты до цоколя лампочки, но не включая лампочку и линзы. Это необработанная мощность или сигнал, которую теперь лампочка и линзы могут излучать и фокусировать сигнал.

## Эквивалентная Изотропно Излучаемая Мощность

*Эквивалентная изотропно излучаемая мощность (ЭИИМ) [Equivalent isotropically radiated power (EIRP)]* - это самая высокая мощность радиосигнала, которая передается с конкретной антенны. Чтобы лучше понять это, рассмотрим наш пример с фонариком. Предположим, что лампочка без линзы вырабатывает мощность 1 Вт. Когда вы устанавливаете линзу в фонарик, она фокусирует этот 1 ватт света. Если бы вы посмотрели на свет сейчас, он казался бы намного ярче. Если бы вы измерили яркость точки света, который создается фонариком, то благодаря эффекту линзы она может быть равна

яркости 8-ваттной лампочки. Таким образом, фокусируя свет, вы можете сделать эквивалентную изотропно излучаемую мощность сфокусированной лампы равной 8 Вт.

Знайте, что вы можете найти другие определения ЭИИМ [EIRP] как **эквивалентная изотропная излучаемая мощность** или **эффективная изотропная излучаемая мощность**. Использование ЭИИМ [EIRP] в этой книге согласуется с определением FCC: «**эквивалентная изотропно излучаемая мощность, произведение мощности, подаваемой на антенну, и коэффициента усиления антенны в заданном направлении относительно изотропной антенны**». Даже когда термины, которые обозначают инициалы, временами отличаются, определение ЭИИМ [EIRP] является **непротиворечивым**.

Как вы узнали ранее в этой главе, антенны способны фокусировать или направлять радиоволновую энергию. Эта способность фокусирования может сделать фактический выходной сигнал антенны намного больше, чем сигнал, поступающий в антенну. Из-за этой способности усиливать выходной радиосигнал регулирующие органы, такие как FCC, ограничивают величину ЭИИМ [EIRP] антенны.

В следующем разделе этой книги вы узнаете, как рассчитать сколько мощности подается на антенну (Расчетный излучатель(IR)) и сколько мощности выйдет от антенны (ЭИИМ(EIRP)).



## Пример из Реальной Жизни

### Почему важны измерения Расчетного Излучателя(IR) и ЭИИМ(EIRP)?

Как вы узнали из главы 1, местная регулирующая организация в отдельной стране или регионе отвечает за регулирование максимальной мощности передачи. FCC и другие регуляторные организации обычно определяют максимальную выходную мощность для расчетного излучателя (IR) и максимальную эквивалентную изотропно излучающую мощность (ЭИИМ(EIRP)), которая излучается антенной. Проще говоря, FCC регулирует максимальное количество энергии, которое поступает в антенну, и максимальное количество энергии, которое выходит из антенны.

Вам нужно знать определение параметров Расчетного Излучателя(IR) и ЭИИМ(EIRP). Однако, экзамен CWNA (CWNA-108) не проверяет вас ни на какие регулирующие мощность правила, так как оно отличается от страны к стране. Вам рекомендуется самим изучить регулирующие правила о максимальной передаваемой мощности той страны, где вы планируете развертывать БЛВС, чтобы не нарушать их. Мощность передачи большинства радиомодулей внутренних Wi-Fi ТД может быть установлена в диапазоне между 1мВт и 100мВт, а большинство радиомодулей Wi-Fi клиентов уже предустановлено в значение из этого диапазона. Таким образом, вам обычно не нужно заботиться о правилах, регулирующих мощность, при установке оборудования БЛВС внутри помещений. Однако, знание нормативных правил, регулирующих мощность, является обязательным при развертывании БЛВС вне помещений.

## Единицы Мощности и Сравнения

При проектировании беспроводной сети 802.11, двумя ключевыми компонентами являются покрытие и производительность. Хорошее понимание радиоволновой мощности, сравнения и радиоматематики может быть очень полезным на этапе проектирования сети.

В следующем разделе, мы представим вам ассортимент *единиц мощности и единиц сравнения*. Важно знать и понимать различные типы единиц измерения и как они соотносятся друг с другом. Некоторые из чисел, с которыми вы будете работать, будут представлять фактические единицы мощности, а другие — относительные единицы сравнения. Фактические единицы мощности представляют собой известные или установленные значения.

Когда мы говорим, что мужчина 6 футового роста – это является примером реального измерения или абсолютного значения. С того момента как рост человека является известным значением, в данном случае 6 футов, вы точно знаете, какой у него рост. Относительные единицы — это сравнительные значения, сравнивающие один элемент с элементом аналогичного типа. Например, если вы хотите сказать кому-то, какой рост у жены мужчины, используя сравнительные единицы измерения, вы можете сказать, что она составляет пять шестых его роста. Теперь у вас есть сравнительные измерения: если вы знаете фактическую высоту одного из них, вы можете определить, насколько высок другой.

Сравнительные единицы измерения полезны при работе с единицами мощности. Как вы увидите далее в этой главе, мы можем использовать эти сравнительные единицы мощности для сравнения области, которую может покрыть одна точка доступа, по сравнению с другой точкой доступа. Используя простую математику, мы можем определить такие вещи, как сколько ватт нужно, чтобы удвоить расстояние сигнала от точки доступа.

Единицы мощности используются для измерения амплитуды передачи и принятой амплитуды. Другими словами, единицы измерения мощности передачи или приема являются *абсолютными измерениями мощности*. Единицы сравнения часто используются для измерения усиления или потерь из-за установки кабеля или антенны. Единицы сравнения также часто представляют разницу по мощности точки А от точки В. Другими словами, единицы сравнения являются мерой *изменения мощности*.

Далее представлен список единиц мощности, используемых в сетях Wi-Fi, за которым следует еще один список единиц для сравнения, все они рассматриваются в следующем разделе:

### Единицы мощности (абсолютные)

- ватт (Вт)
- милливатт (мВт)
- децибелы относительно 1 милливатта (дБм)

### Единицы сравнения (относительные)

- децибел (дБ)
- децибелы относительно изотропного излучателя (дБи)
- децибелы относительно полуволновой дипольной антенны (дБд)

## Ватт

*Ватт [watt] (Bm[W])* - базовая единица мощности, названная в честь Джеймса Ватта, шотландского изобретателя 18 века. Один ватт равен 1 амперу тока протекающему при 1 вольте. Чтобы дать лучшее объяснение ватта, мы будем использовать модификацию классической аналогии с водой.

Многие из вас наверняка знакомы с такой техникой, как минимойка. Для тех, кто не знаком с ней, это машина, которая подключается к источнику воды, как например садовый шланг, и позволяет вам направить струю воды высокого давления на объект, предполагая, что быстро движущаяся вода очистит объект. Успех минимойки основан на двух компонентах: давлении воды и объеме воды, использованном за определенный период времени, также называемых как поток. Эти две составляющие обеспечивают мощность водного потока. Если вы увеличите давление, вы увеличите мощность потока. Если вы увеличите поток воды, вы также увеличите силу потока. Мощность потока равна произведению давления на поток.

Ватт очень похож на выход минимойки высокого давления. Вместо давления, создаваемого машиной, в электрической системе – напряжение. Вместо водяного потока, в электрической системе ток, который измеряется в амперах. Таким образом, количество генерируемых ватт равно произведению вольт на ампер.

## Милливатт

*Милливатт (mWt)* является также единицей мощности. Проще говоря, милливатт равен 1/1000 ватта. Причина, по которой вам нужно беспокоиться о милливаттах, заключается в том, что большая часть внутреннего оборудования 802.11, которое вы будете использовать, передает с уровнями мощности от 1 мВт до 100 мВт. Вспомните, что уровень мощности передачи радиомодуля будет ослаблен любым кабелем и будет усилен антенной. Хотя регулирующие организации, такие как FCC могут разрешить выходную мощность расчетного излучателя (IR) до 1 ватта, только в редких случаях в соединениях точка-точка, таких как канал связи типа мост здание-здание, вы можете использовать оборудование 802.11 с мощностью передачи более 300 мВт.



### Пример из Реальной Жизни

#### Что представляют собой настройки мощности передачи у производителей Wi-Fi?

Все производители Wi-Fi предлагают возможность настройки параметров мощности передачи точки доступа. Радиомодуль типовой ТД обычно имеет мощность передачи от 1мВт до 100мВт. Однако, не все производители Wi-Fi представляют значение мощности передачи одним и тем же способом. Настройки мощности передачи большинства производителей представляют Расчетный излучатель(IR), в то время как настройки мощности передачи других производителей вместо этого в действительности могут быть ЭИИМ (EIRP). Кроме того, производители Wi-Fi могут также указывать амплитуду передачи либо в мВт, либо в дБм - например, 32мВт или +15дБм - еще некоторые могут просто показывать мощность передачи в виде значений процентов, например: 32 процента. Вам нужно обратиться к руководству по установке вашего конкретного производителя Wi-Fi, чтобы полностью понимать значение амплитуды передачи.

## Децибел

Первое, что вы должны знать про *децибел (dB)* [*decibel (dB)*] - это то, что это единица сравнения, а не единица мощности. Следовательно, она используется чтобы представить разницу между двумя величинами. Другими словами, dB - это относительное выражение и мера изменения мощности.

В беспроводных сетях децибелы часто используются или для сравнения мощности двух передатчиков, или, что более часто, для сравнения разницы или потерь между выходным ЭИИМ (EIRP) передающей антенны и количеством принимаемой мощности приемной антенны.

Децибел получено из термина *бел [bell]*. Сотрудникам Телефонной Лаборатории Белла [Bell Telephone Laboratories] нужен был способ представить потери мощности на телефонных линиях в виде отношения мощностей. Они дали определение, что бел - это отношение 10 к 1 между мощностью двух звуков. Давайте рассмотрим пример. Точка доступа передает данные со 100мВт. Ноутбук1 принимает сигнал от ТД с уровнем мощности 10мВт, а ноутбук2 принимает сигнал от ТД с уровнем мощности 1мВт.

Разница между сигналом точки доступа (100мВт) и ноутбуком1 (10мВт) является 100:10, или 10:1, или 1 бел.

Разница между сигналом от ноутбук1 (10мВт) и ноутбук2(1мВт) является также отношением 10:1, или 1 бел. Таким образом разница по мощности между точкой доступа и ноутбук2 является 2 бела.

Белы можно рассматривать математически, используя логарифмы. Не все понимают или помнят логарифмы, поэтому мы их повторим. Во-первых, нам нужно рассмотреть возведение числа в степень. Если вы возьмете 10 и возведете ее в третью степень ( $10^3 = y$ ), то то что вы делаете на самом деле - это умножаете три 10ки ( $10 \times 10 \times 10$ ). Если вы проведете математические операции, вы вычислите что  $y$  равен 1000. Таким образом решение  $10^3 = 1,000$ . При вычислении логарифма, вы меняете формулу на  $10^y = 1,000$ . Здесь вы пытаетесь вычислить в какую степень нужно возвести 10, чтобы получить 1000. Из этого примера вы знаете, что ответ 3. Вы можете также записать это уравнение как  $y=\log_{10}(1000)$  или  $y=\log_{10}1000$ . Таким образом полное уравнение это  $3=\log_{10}1000$ . Ниже даны несколько примеров формул степеней и логарифмов.

---

$10^1 = 10$	$\log_{10}(10) = 1$
$10^2 = 100$	$\log_{10}(100) = 2$
$10^3 = 1,000$	$\log_{10}(1,000) = 3$
$10^4 = 10,000$	$\log_{10}(10,000) = 4$

---

Теперь давайте вернемся обратно и вычислим белы от точки доступа до ноутбука2, например, используя логарифмы. Помните, что белы используются чтобы вычислить отношение между двумя мощностями. Давайте обозначим мощность точки доступа как  $P_{AP}$ , а мощность ноутбука2 как  $P_{L2}$ . Тогда формула для этого примера будет  $y=\log_{10}(P_{AP}/P_{L2})$ . Если в формулу подставить значения мощностей, то формула станет  $y=\log_{10}(100/1)$ , или  $y=\log_{10}(100)$ . То есть уравнение спрашивает, 10 введенное в какую степень равно 100? Ответ 2 бела ( $10^2=100$ ).

Хорошо, но это должен быть раздел о децибелях, а пока мы рассмотрели только белы. В определенных условиях белы недостаточно точны, поэтому вместо этого мы используем децибели. Децибел равен 1/10 бела. Чтобы вычислить децибели, все что вам нужно сделать это умножить белы на 10. Таким образом формулы для белов и децибелов следующие:

$$\text{белы} = \log_{10} \left( \frac{P_1}{P_2} \right)$$

$$\text{децибели} = 10 \times \log_{10} \left( \frac{P_1}{P_2} \right)$$

Теперь вернемся назад и посчитаем децибели на примере точки доступа к ноутбуку2. Теперь формула  $y=10 \times \log_{10}(P_{AP}/P_{L2})$ . Если подставить значение мощности, то формула примет вид  $y=10 \times \log_{10}(100/1)$ , или  $y=10 \times \log_{10}(100)$ . То есть ответ +20 децибел. +20 децибел равно +2 бела.



Для экзамена CWNA вам не нужно знать, как считать логарифмы. Эти примеры здесь только для того, чтобы дать вам некоторое базовое понимание того, чем они являются, и как их считать. Позже в этой главе, вы узнаете, как считать децибели без использования логарифмов.

Теперь, когда вы узнали о децибелях, вы, вероятно, все еще задаетесь вопросом, почему вы не можете работать только с милливаттами. Вы можете, если хотите, но поскольку изменения мощности рассчитываются с использованием логарифмических формул, различия между значениями могут стать чрезвычайно большими, и с ними будет сложнее иметь дело. Легче сказать, что сигнал мощностью 100 мВт уменьшился на 70 децибел, чем сказать, что он уменьшился до 0,00001 мВт. Из-за масштаба чисел вы можете понять, почему с децибелями легче работать.



## Пример из Реальной Жизни

### Почему Вам Следует Использовать Децибели?

Как вы узнали из Главы 3, многие модели поведения распространения могут негативно повлиять на волну. Одна из таких моделей поведения распространения, которую вы узнали, это затухание на пути в свободном пространстве.

Если точка доступа 2,4ГГц передает со 100мВт, а ноутбук находится в 100 метрах (0,1 километре) от точки доступа, ноутбук принимает только около 0,000001 милливатт мощности. Разница между числами 100 и 0,000001 настолько велика, что не имеет большого значения для того, кто на нее смотрит. Кроме того, можно случайно пропустить ноль при написании или вводе 0,00001 (как мы только что сделали).

Если использовать формулу потерь на пути в свободном пространстве (FSPL) для вычисления децибелов потерь для этого сценария, то формула будет следующей:

$$\text{децибелы} = 32,4 + 20\log_{10}(2400) + 20\log_{10}(0,1)$$

Ответ - потери 80,004 dB, то есть примерно 80 децибел потеря. С этим числом проще работать и менее вероятно некорректно напечатать.

## Децибелы относительно Изотропного Излучателя (дБи)

Ранее в этой главе мы сравнили антенну с изотропным излучателем. Теоретически изотропный излучатель может излучать одинаковый сигнал во всех направлениях. Антenna не может этого сделать из-за конструктивных ограничений. В других случаях вы не хотите, чтобы антenna излучала во всех направлениях, потому что вы хотите сфокусировать сигнал антенны в определенном направлении. В любом случае необходимо уметь рассчитать мощность излучения антенны, чтобы можно было определить, насколько силен сигнал на определенном расстоянии от антенны. Вы можете также захотеть сравнить выходную мощность одной антенны с другой.

Усиление, или увеличение мощности от антенны по сравнению с тем, что генерирует изотропный излучатель, называется, как *изотропные децибелы (дБи)* [*decibels isotropic (dBi)*]. Перефразируя по-другому - это *усиление в децибелах по отношению к изотропному излучателю или изменение по мощности относительно антенны*. Так как антенны измеряются по *усиленнию*, а не *мощности*, вы можете сделать заключение что дБи - это относительная мера, а не абсолютная мера мощности. дБи - это просто мера или параметр усиления антенны. Величина дБи измеряется в самой сильной точке, или в точке фокуса, сигнала антенны. Поскольку антенны всегда фокусируют свою энергию больше в одном направлении, чем в другом, значение дБи антенны всегда является положительным усилением, а не потерями. Существуют, однако, антенны со значением дБи равным 0, которые часто называются антеннами без усиления или антенны с единичным усилением.

Обычной антенной, используемой в точках доступа, является полуволновая дипольная антenna. Полуволновая дипольная антenna представляет собой небольшую, обычно в резиновом или пластиковом корпусе, всенаправленную антенну общего пользования. А 2,4 ГГц полуволновая дипольная антenna имеет значение дБи 2,14.



Каждый раз, когда вы видите дБи, думайте об *усилении антенны*.

## Децибелы относительно полуволновой дипольной антены (дБд)

Индустрия антенн использует две шкалы дБ, чтобы описать усиление антенн. Первая шкала, о которой вы узнали, это дБи, которая используется, чтобы описать усиление антены относительно теоретического изотропной антены. Другая шкала используется, чтобы описать усиление антены – это *децибелы диполя*, или *усиление в децибелах относительно дипольной антены*. Так значение дБд – это увеличение в усиении антены, когда она сравнивается с сигналом дипольной антены. Как вы знаете из Главы 5, дипольные антенны являются также и всенаправленными [omnidirectional] антеннами. Следовательно, значение дБд – это мера усиления всенаправленной антены, а не усиление односторонней антены.

Так как дипольные антенны измеряются по *усиленнию*, а не по *мощности*, вы также можете заключить, что дБд – это относительная мера, а не мера мощности.

Определение дБд кажется достаточно простым, но что произойдет, когда вы захотите сравнить две антенны, и одна представлена в дБи, а другая в дБд? Это действительно очень просто. Стандартная дипольная антenna имеет значение дБи



Не забывайте, что дБ, дБи и дБд являются сравнительными, или относительными мерами, а не единицами мощности.



## Пример из Реальной Жизни

### Настоящая сенсация про дБд

При работе с оборудованием стандарта 802.11 маловероятно, что у вас будет антенна со значением дБд. Антенны 802.11 обычно измеряются с использованием дБи. В тех редких случаях, когда вы сталкиваетесь с антенной, измеряемой в дБд, просто добавьте 2,14 к значению дБд, и вы узнаете значение антенны в дБи.

## Децибелы относительно 1 Милливатта (дБм)

Ранее, когда вы читали про белы и децибелы, вы узнали, что они измеряют разницу или отношение между двумя сигналами. Независимо от типа передаваемой мощности, все, что вы действительно знали, это то, что один сигнал был больше или меньше другого на определенное количество белов или децибелов. дБм также представляет сравнение, но вместо сравнения сигнала с другим сигналом он используется чтобы сравнить сигнал с 1 милливаттом мощности. дБм означает *децибелы относительно 1 милливатта*. Итак, что вы делаете - это выставляете дБм в 0 (ноль) и приравниваете это к 1 милливатту мощности. Так как дБм - это мера, которая сравнивает с известной величиной, 1 милливатт, то в действительности она является мерой абсолютной мощности. Так как децибелы (относительные значения) сравниваются с 1 милливаттом (абсолютное значение), рассматривайте дБм как абсолютную оценку, которая измеряет изменение мощности относительно 1 милливатта. Теперь вы можете утверждать, что 0дБм равно 1 милливатту. Используя формулу  $\text{дБм} = 10 \times \log_{10}(P_{\text{мВт}})$ , вы можете определить, что 100мВт мощности равно +20дБм.

Если случится, что у вас будет значение дБм устройства и вы захотите вычислить соответствующее значение в милливаттах, вы это тоже сможете сделать. Формула  $P_{\text{мВт}} = 10^{(\text{дБм}/10)}$ .

Помните, что 1 милливатт является точкой отсчета, а 0 дБм равен 1 мВт. Любое значение абсолютной мощности в +дБм указывает на амплитуду более 1 мВт. Любое значение абсолютной мощности в -дБм указывает на амплитуду менее 1 мВт. Например, ранее мы говорили, что амплитуда передачи большинства радиомодулей стандарта 802.11 обычно находится в диапазоне от 1 мВт до 100 мВт. Амплитуда передачи 100 мВт равна +20 дБм. Из-за потерь на пути в свободном пространстве, принимаемый сигнал будет всегда меньше 1 мВт. Очень сильный принимаемый сигнал это -40дБм, что эквивалентно 0,0001 мВт (1/10 000ая от 1 милливатта).

Может показаться странным иметь дело и с милливаттами, и с дБм. Если милливатты являются допустимой мерой мощности, почему не использовать их? Почему

вы должны или хотите также использовать дБм? Это хорошие вопросы, которые часто задаются студентами. Одна причина - это просто, что абсолютные значения в дБм часто легче понять, чем значения в миллионных и миллиардных долях одного милливатт. Большинство радиомодулей 802.11 распознают принимаемый сигнал от -30дБм (1/1000 ая от 1 мВт) до -100 дБм (1/10 миллиардной от 1 милливатта). Человеческий мозг может осознать -100дБм намного проще, чем 0,000000001 милливатт. Во время радиоисследования, инженеры БЛС всегда определяют зону покрытия, записывая силу принимаемого сигнала в величинах дБм.

Другая очень практическая причина использования дБм может быть показана снова с помощью формулы потерь на пути в свободном пространстве (FSPL). Ниже даны два уравнения FSPL. Первое уравнение вычисляет потери в децибелах 2,4ГГц сигнала на 100 метрах (0,1 километра) от источника радиосигнала, а вторая вычисляет потери в децибелах 2,4ГГц сигнала на 200 метрах (0,2 километра) от источника радиосигнала:

$$\text{FSPL} = 32,4 + 20\log_{10}(2400) + 20\log_{10}(0,1) = 80,00422 \text{ дБ}$$

$$\text{FSPL} = 32,4 + 20\log_{10}(2400) + 20\log_{10}(0,2) = 86,02482 \text{ дБ}$$

В этом примере, удваивая расстояние от радиоисточника, сигнал уменьшался примерно на 6 дБ. Если вы удвоите расстояние между передатчиком и приемником, принимаемый сигнал уменьшится на 6дБ. Не важно какие числа выбраны, если расстояние удвоено, потеря в децибелах составит 6 дБ. Это правило также подразумевает, что, если вы увеличите амплитуду на 6дБ, расстояние, когда еще возможен прием, удвоится. Это правило 6дБ очень полезно для сравнения размеров зон покрытия или оценки покрытия передатчика. Правило 6дБ также полезно для понимания усиления антенны, потому что каждые дополнительные 6дБ усиления антенны будет удваивать дистанцию полезного радиосигнала. Запомните, если вы работаете с милливаттами, то это правило не подходит. Конвертируя милливатты в дБм, вы получаете более простой способ для сравнения сигналов.



**Запомните правило 6дБ: +6дБ удваивает дистанцию полезного сигнала; -6дБ уполовинивает дистанцию полезного сигнала.**

Использование дБм делает простым вычисление влияния усиления антенны на сигнал. Если передатчик генерирует сигнал +20дБм, а антенна добавляет 5дБи усиления сигнала, то мощность, которая излучается антенной (ЭИИМ(EIRP)) равна сумме двух чисел, то есть +25дБм.

## Закон Обратных Квадратов

Вы только что узнали о правиле 6дБ, которое гласит, что изменение на +6дБ в сигнале удваивает полезную дистанцию сигнала, а изменение на -6дБ сигнала уполовинивает полезную дистанцию сигнала. Это правило и эти числа основаны на законе обратного квадрата, изначально открытого Исааком Ньютона.

Этот закон гласит, что изменение в мощности равно 1 поделенной на квадрат изменения расстояния. Другими словами, если расстояние от источника сигнала удвоить, то энергия распределиться по области в четыре раза большей, в результате получая одну-четвертую от начальной интенсивности сигнала.

Это означает, что если вы принимаете сигнал на определенном уровне мощности и на

**136 Глава 4 • Компоненты, Параметры и Математика Радиосвязи**  
определенном расстоянии (D), и вы удвоите расстояние (изменение в расстоянии = 2),  
новый уровень мощности изменится на  $1/(2)^2$ . Чтобы использовать этот принцип для  
расчета ЭИИМ(EIRP) на определенном расстоянии, используется формула  $P/(4\pi \times r^2)$ , где  
Р равно начальной мощности ЭИИМ(EIRP), а г равно исходному (опорному) расстоянию.

Давайте также рассмотрим формулы для потерь на пути в свободном пространстве:

$$\text{FSPL} = 36,6 + 20 \log_{10}(F) + 20 \log_{10}(D)$$

FSPL = потери на пути в dB

F = частота в МГц

D = расстояние в милях между антеннами

$$\text{FSPL} = 32,4 + 20 \log_{10}(F) + 20 \log_{10}(D)$$

FSPL = потери на пути в dB

F = частота в МГц

D = расстояние в километрах между антеннами

Концепция FSPL (потерь на пути в свободном пространстве) также основана на законе обратных квадратов Ньютона. Основная переменная для закона обратных квадратов это просто расстояние. Формула FSPL также базируется на расстоянии, но включает еще другую переменную: частоту.

## Радиоволновая математика

При обсуждении темы Радиоволновой математики, большинство людей ёжится и паникует, потому что они ожидают формулы, в которых есть логарифмы. Не бойтесь. Вы скоро узнаете радиоволновую математику без использования логарифмов. Если вы хотите освежить некоторые ваши математические навыки перед прохождением этого раздела, то просмотрите следующее:

- Сложение и вычитание с использованием чисел 3 и 10
- Умножение и деление с использованием чисел 2 и 10

Нет, мы не шутим. Если вы знаете как прибавить и вычесть, используя 3 и 10, и как умножить и разделить, используя 2 и 10, то вы имеете все необходимые математические навыки, чтобы выполнять радиоволновую математику. Читайте, и мы научим вас как.

## Правило 10-ти и 3-х

До того, как вы полностью погрузитесь в *правило 10-ти и 3-х*, важно знать, что это правило не может дать вам точно такие же ответы, которые вы получили бы, если бы использовали логарифмические формулы. Правило 10-ти и 3-х дает примерные значения, не обязательно точные значения. Если вы инженер, создающий продукт, который должен соответствовать регуляторным радиочастотным правилам, вам нужно использовать логарифмы, чтобы вычислить точные значения. Однако, если вы сетевой дизайнер, проектирующий сеть для вашей компании, то вы найдете, что правило 10-ти и 3-х даст вам числа и точность, которые вам нужны для правильного планирования вашей сети.

Этот раздел научит вас основным вычислениям. Все вычисления будут базироваться на следующих четырех правилах 10-ти и 3-х:

- Каждые 3 дБ усиления (относительного), удваивают абсолютную мощность (мВт).
- Каждые 3 дБ потерь (относительных), уменьшают вдвое абсолютную мощность (мВт).
- Каждые 10 дБ усиления (относительного), умножают абсолютную мощность (мВт) на 10.
- Каждые 10 дБ потерь (относительных), делят абсолютную мощность (мВт) на 10.

Например, если ваша точка доступа настроена на передачу 100 мВт, а антенна рассчитана на 3дБи пассивного усиления, то величина мощности, которая будет излучаться антенной (ЭИИМ (EIRP)) будет 200 мВт. Следуя правилу, которое вы только что узнали, вы увидите, что 3дБ усиления антенны привело к удвоению сигнала мощностью 100 мВт от точки доступа. И наоборот, если ваша точка доступа настроена на передачу на уровне 100 мВт и подключена к кабелю, в котором потери составляют 3 дБ, величина абсолютной амплитуды на конце кабеля составит 50 мВт. Здесь вы можете видеть, что 3 дБ потерь в кабеле привели к тому, что сигнал мощностью 100 мВт от точки доступа уменьшился вдвое.

В другом примере, если ваша точка доступа настроена на передачу с мощностью 40 мВт, а антенна рассчитана на пассивное усиление 10 дБи, мощность, излучаемая антенной (ЭИИМ(EIRP)), составит 400 мВт. Здесь вы можете видеть, что усиление антенны на 10 дБ привело к увеличению сигнала мощностью 40 мВт от точки доступа в 10 раз. И наоборот, если ваша точка доступа настроена на передачу 40 мВт и подключена к кабелю, который вносит 10 дБ потерь, величина абсолютной амплитуды на конце кабеля составит 4 мВт. Здесь вы можете видеть, что 10 дБ потерь в кабеле привели к тому, что 40 мВт сигнал от точки доступа уменьшился на 10.

Если вы запомните эти правила, вы сможете быстро выполнять радио вычисления. После знакомства с этими правилами, посмотрите на Упражнение 4.1, которое проведет вас через пошаговую процедуру использования правила 10-ти и 3-х. По мере выполнения работ по шагам, помните, что дБм — это единица мощности, а дБ — это единица изменения. дБ — это значение изменения, которое может быть применено к дБм. Если у вас есть сигнал +10 дБм и он увеличивается на 3дБ, то вы можете сложить эти два числа вместе и получить в результате сигнал +13дБм.

**УПРАЖНЕНИЕ 4.1****Пошаговое Использование Правила 10-ти и 3-х.**

1. На листе бумаги сделайте две колонки. Заголовок первой колонки должен быть **дБм**, заголовок второй колонки должен быть **мВт**.

дБм	мВт
-----	-----

2. Рядом с заголовком дБм поставьте знаки + и -, а рядом с заголовком мВт поставьте знаки × и знаки ÷.

Это поможет вам запомнить, что любая математическая операция в колонке дБм может быть только сложение или вычитание, а любая математическая операция в колонке мВт может быть только умножение или деление.

+	×
-	÷
дБм	мВт

3. Слева от знаков + и - напишите числа **3** и **10**, а справа от знаков × и ÷ напишите числа **2** и **10**.  
Любое сложение или вычитание в колонке дБм может быть выполнено только с использованием чисел 3 и 10. Любое умножение или деление в колонке мВт может быть выполнено только с использованием чисел 2 и 10.

3    +	×    2
10    -	÷    10
дБм	мВт

4. Если есть + слева, должен быть × справа. Если есть – слева, должно быть ÷ справа.  
5. Если вы добавляете или вычитаете 3 слева, вы должны умножить или разделить на 2 справа. Если вы добавляете или вычитаете 10 слева, вы должны умножить или разделить на 10 справа.  
6. Последняя вещь, которую вам нужно сделать – это записать **0** под колонкой дБм и **1** под колонкой мВт.

Помните, определение дБм – это *децибелы относительно 1 милливатта*. То есть диаграмма теперь показывает, что 0 дБм равно 1 милливатту.

3    +	×    2
10    -	÷    10
дБм	мВт
0	1

Прежде чем мы продолжим с примером, необходимо подчеркнуть, что изменение на ±3 дБ соответствует удвоению или уменьшению вдвое мощности, независимо от того, какая мера мощности используется. В нашем случае использования правила 10-ти и 3х, мы имеем дело с милливаттами, потому что это типичное измерение амплитуды передачи, используемое с оборудованием 802.11.

Однако, важно помнить, что увеличение на +3 дБ означает удвоение мощности независимо от используемой шкалы. То есть увеличение на +3дБ 1,21 гигаватта мощности даст 2,42 гигаватта мощности.



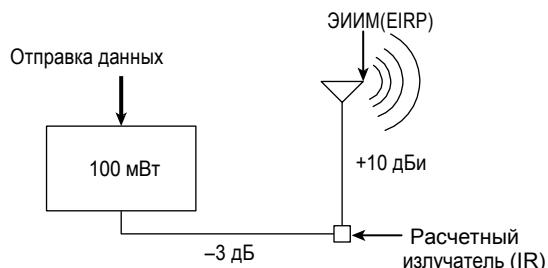
Анимированное объяснение правила 10 и 3 вместе с примерами было создано с помощью Microsoft PowerPoint, и может быть загружено с онлайн ресурса этой книги ([www.wiley.com/go/cwnasg6e](http://www.wiley.com/go/cwnasg6e)). Имена файлов PowerPoint следующие:

- 10s and 3s Template.ppt
- Rule of 10s and 3s Example 1.ppt
- Rule of 10s and 3s Example 2.ppt
- Rule of 10s and 3s Example 3.ppt
- Rule of 10s and 3s Example 4.ppt

#### УПРАЖНЕНИЕ 4.2

##### Пример Правила 10-ти и 3-х

У вас есть беспроводной мост, который генерирует 100мВт сигнала. Мост подключен к антенне кабелем, который вносит потери сигнала -3дБ. Антенна дает усиление сигнала +10дБи. В этом примере, вычислите мощность в точке расчетного излучателя (IR) и ЭИИМ (EIRP).



Напоминаем, как показано на рисунке, IR — это сигнал до антенны, но не включая ее, а ЭИИМ(EIRP) — это сигнал, излучаемый антенной.

1. Первый шаг это определить использовать 10 или 2, и × или ÷ , вы можете пойти от 1мВт до 100мВт.

Нетрудно понять, что, если дважды умножить 1 на 10, получится 100. То есть мост генерирует 100мВт, или +20дБм мощности.

3	+			×	2
10	-			÷	10
		<u>дБм</u>		<u>мВт</u>	
		0		1	
+ 10		10		10	× 10
+ 10		20		100	× 10

2. Далее у вас есть антенный кабель, который вносит -3дБ потерь в сигнал. Уменьшение на 3дБ в колонке дБм соответствует делению колонки мВт на 2. После того, как вы рассчитаете эффект потери -3 дБ, вы узнаете значение IR. Вы можете представить IR как +17дБм или как 50мВт.

3	+			×	2
10	-			÷	10
		<u>дБм</u>		<u>мВт</u>	
		0		1	
+ 10		10		10	× 10
+ 10		20		100	× 10
- 3		17		50	÷ 2

3. Все что остается сделать, это только рассчитать усиление сигнала за счет усиления антенны. Так как усиление 10дБи, вы добавляете 10 в колонке дБм и умножаете на 10 в колонке мВт. Это даст вам ЭИИМ (EIRP) +27дБм, или 500 мВт.

3	+			×	2
10	-			÷	10
		<u>дБм</u>		<u>мВт</u>	
		0		1	
+ 10		10		10	× 10
+ 10		20		100	× 10
- 3		17		50	÷ 2
+ 10		27		500	× 10

---

Числа, выбранные в примере, были простыми, с использованием значений, которые являются частью шаблона. Однако, в реальном мире этого не будет. Применив немного креативности, вы можете вычислить усиление или затухание для любого целого числа. К сожалению, правило 10 и 3 не работает для дробных или десятичных чисел. Для этих чисел, вам нужно использовать логарифмическую формулу.

Усиление или затухание в дБ являются кумулятивными. Если, например, у вас есть три куска кабеля соединяющих приемопередатчик с антенной, и каждый кусок кабеля дает 2дБ потерь, все три кабеля создадут 6дБ потерь. Используя правило 10-ти и 3-х, вычитание 6 дБ равносильно вычитанию 3дБ дважды. Децибелы очень гибкие. До тех пор, пока вы приходите с той суммой, которая вам нужна, им все равно, как вы это сделаете.

Таблица 4.1 показывает, как вычислить все целые числа дБ потерь и усиления от -10 до +10 используя комбинацию 10-ти и 3-х. Найдите минутку, чтобы посмотреть на эти значения, и вы поймете, что, проявив немного творчества, вы можете вычислить потери или усиление любого целого числа.

**ТАБЛИЦА 4.1** потери и усиление в дБ ( от -10 до +10)

Потери или усиление(дБ)	Комбинация 10 и 3
-10	-10
-9	-3 -3 -3
-8	-10 -10 +3 +3 +3 +3
-7	-10 +3
-6	-3 -3
-5	-10 -10 +3 +3 +3 +3 +3
-4	-10 +3 +3
-3	-3
-2	-3 -3 -3 -3 +10
-1	-10 +3 +3 +3
+1	+10 -3 -3 -3
+2	+3 +3 +3 +3 -10
+3	+3
+4	+10 -3 -3
+5	+10 +10 -3 -3 -3 -3 -3
+6	+3 +3
+7	+10 -3
+8	+10 +10 -3 -3 -3 -3
+9	+3 +3 +3
+10	+10

## Краткий итог радиоволновой математики

Всегда помните, что в итоге вы пытаетесь вычислить мощность в разных точках радиоволновой системы и эффекты вызванные усилением или потерями. Если вы хотите произвести радиоволновые математические вычисления с использованием логарифмических формул, то вот они:

$$\text{дБм} = 10 \times \log_{10} (P_{\text{мВт}})$$

$$\text{мВт} = 10^{(\frac{\text{дБм}+10}{10})}$$

Если вы хотите использовать правило 10-ти и 3х, просто запомните эти четыре простых задачи, и у вас не будет проблем:

- 3 дБ усиления = мВт × 2
- 3 дБ потеря = мВт ÷ 2
- 10 дБ усиления = мВт × 10
- 10 дБ потеря = мВт ÷ 10

Таблица 4.2 представляет собой краткое справочное руководство по сравнению величин абсолютной мощности в милливаттах с абсолютной мощностью списка значений в дБм.

**ТАБЛИЦА 4.2** Преобразование дБм и мВт

дБм	мВт	Уровень мощности
+36 дБм	4,000 мВт	4 ватта
+30 дБм	1,000 мВт	1 ватт
+20 дБм	100 мВт	1/10ая 1 ватта
+10 дБм	10 мВт	1/100ая 1 ватта
0 дБм	1 мВт	1/1,000ая 1 ватта
-10 дБм	0.1 мВт	1/10ая 1 милливатта
-20 дБм	0.01 мВт	1/100ая 1 милливатта
-30 дБм	0.001 мВт	1/1,000ая 1 милливатта
-40 дБм	0.0001 мВт	1/10,000ая 1 милливатт
-50 дБм	0.00001 мВт	1/100,000ая 1 милливатта
-60 дБм	0.000001 мВт	1 миллионная 1 милливатта

(Продолжается)

**ТАБЛИЦА 4.2** Преобразование дБм и мВт (продолжение)

дБм	мВт	Уровень мощности
-70 дБм	0.0000001 мВт	1 десятимиллионная 1 милливатта
-80 дБм	0.00000001 мВт	1 стомиллионная 1 милливатта
-90 дБм	0.000000001 мВт	1 миллиардная 1 милливатта

## Уровень шума

*Уровень шума* - это окружающий или фоновый уровень энергии радиоволн на конкретном канале. Эта фоновая энергия может включать модулированные или кодированные биты, приходящие от соседних, передающих в стандарте 802.11, радиомодулей, или немодулированная энергия приходящая от не 802.11 устройств, таких как микроволновые печи, Bluetooth устройства, радиотелефоны, и так далее. Все электромагнитное имеет потенциал к увеличению амплитуды уровня шума на конкретном канале.

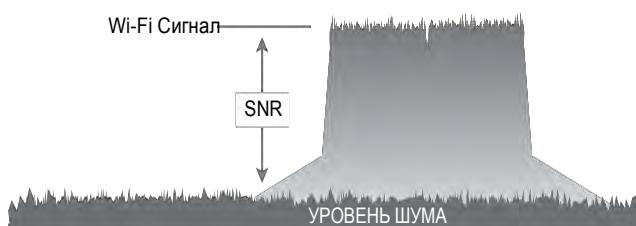
Амплитуда уровня шума, которую иногда называют «фоновый шум», различается в разных средах. Например, уровень шума 2,4 ГГц промышленного, научного и медицинского (ISM) канала может быть около -100 дБм в обычной среде. Однако, в более шумной радио среде, такой как завод, может иметь уровень шума -90 дБм, из-за электрических машин(станков), работающих на заводе. Также стоит заметить, что уровень шума 5ГГц каналов почти всегда ниже уровня шума 2,4 ГГц каналов, потому что полосы 5ГГц частот менее заполнены.

## Отношение Сигнал-Шум (SNR)

Многие производители Wi-Fi определяют качество сигнала как отношение *сигнал-шум* [*signal-to-noise ratio (SNR)*]. Как показано на Рисунке 4.2, SNR – это разница в децибелах между принимаемым сигналом и фоновым уровнем шума, т.е. в действительности – это не отношение.

**РИСУНОК 4.2**

Отношение Сигнал-Шум



Например, если радиомодуль принимает сигнал  $-85$  дБм, а уровень шума измеряется в  $-100$  дБм, разница между принимаемым сигналом и фоновым шумом составит  $15$  дБ. SNR равен  $15$  дБ.

Передача данных может быть повреждена из-за очень низкого SNR. Значит, если амплитуда уровня шума очень близка к амплитуде принимаемого сигнала, то вероятнее всего произойдет повреждение данных, и это приведет к повторным передачам на 2ом уровне. Повторные передачи (или ретранзиты) негативно влияют и на пропускную способность, и на задержку. Отношение сигнал-шум (SNR) в  $25$  дБ или больше считается сигналом хорошего качества, а SNR в  $10$  дБ или ниже считается сигналом с очень слабым качеством.

## Отношение Сигнал к Помехе плюс Шум (SINR).

Годами SNR был стандартным показателем сетей Wi-Fi. За последние несколько лет, появился термин *отношение сигнал-к-помехе-плюс-шум (signal-to-interference-plus-noise ratio (SINR))*, и используется производителями. SINR – это разница между мощностью основного радиосигнала, по сравнению с суммой мощности радио помехи и фонового шума. Эта разница измеряется в децибелах.

SNR, как правило, является значением, которое трактуется и рассматривается за промежуток времени, так как радиоволновой уровень фонового шума имеет тенденцию быть отчасти постоянным в течении времени. SINR, однако, соотносит основной радиосигнал с помехой(интерференцией) и шумом. В то время как уровень шума, как правило, не сильно флюктуирует, помехи от других устройств скорее всего будут наиболее обычным и частым явлением.

Поскольку интерференция может происходить более часто, SINR является более лучшим показателем того, что происходит в определенное время.

## Индикатор Силы Принимаемого Сигнала (RSSI)

*Чувствительность приема* указывает на уровень мощности радиосигнала, требуемый для успешного приема радиоприемником. Чем ниже уровень мощности, который приемник может успешно обработать, тем лучше чувствительность приема. Думайте об этом, как если бы вы были на игре в хоккей. Есть окружающий уровень шума, который исходит от всего, что вас окружает. Есть определенная громкость, с которой вы должны говорить с соседями, чтобы вас услышали. Этот уровень – чувствительность приема. Это самый слабый сигнал, который приемопередатчик может декодировать при нормальных условиях. При этом, если шум в определенной области громче обычного, то минимальный уровень, на котором вы должны говорить или кричать, увеличивается, чтобы ваш сосед вас услышал и понял.

В оборудовании БЛВС, приемная чувствительность обычно определяется как функция от скорости сети. Производители Wi-Fi обычно указывают свои пороги приемной чувствительности для различных скоростей передачи данных; пример спецификации одного производителя для  $2,4$  ГГц радио перечислены в Таблице 4.3. Для любого конкретного приемника, для поддержки более высокой скорости передачи данных требуется большая

мощность для приемного радиомодуля. Различные скорости используют различные техники модуляции и способы кодирования, а более высокие скорости передачи данных используют методы кодирования, которые более подвержены искажениям. Более низкие скорости передачи данных используют методы модуляции-кодирования, которые менее подвержены искажениям.

Скорость передачи данных	Амплитуда принимаемого сигнала
MCS7	-77 дБм
MCS6	-78 дБм
MCS5	-80 дБм
MCS4	-85 дБм
MCS3	-88 дБм
MCS2	-90 дБм
MCS1	-90 дБм
MCS0	-90 дБм
54 Мбит/с	-79 дБм
48 Мбит/с	-80 дБм
36 Мбит/с	-85 дБм
24 Мбит/с	-87 дБм
18 Мбит/с	-90 дБм
12 Мбит/с	-91 дБм
9 Мбит/с	-91 дБм
6 Мбит/с	-91 дБм

Стандарт 802.11-2020 определяет *индикатор силы принятого сигнала [received signal strength indicator (RSSI)]* как относительную метрику, используемую радиомодулями 802.11, чтобы измерить силу(амплитуду) сигнала. Параметр измерения 802.11 RSSI может иметь значение от 0 до 255. Значение RSSI создано для использования производителями оборудования БЛВС в качестве относительной меры мощности радиосигнала, который принимается радиомодулем 802.11. Значения RSSI обычно сопоставляют с порогами приемной чувствительности, выраженными в абсолютных значениях дБм, как показано в Таблице 4.4.

Например, показатель RSSI равный 30 может обозначать -30 дБм амплитуды принимаемого сигнала. Показатель RSSI равный 0 может соответствовать -110 дБм амплитуды принимаемого сигнала. Другой производитель может использовать параметр RSSI равный 255, чтобы представить -30 дБм амплитуды принимаемого сигнала, и 0, чтобы обозначить -100 дБм амплитуды принимаемого сигнала.

**ТАБЛИЦА 4.4** Значения индикатора силы принимаемого сигнала (RSSI) (пример от производителя)

RSSI	Порог приемной чувствительности	Сила сигнала (%)	Отношение сигнал-шум	Качество сигнала(%)
30	-30 дБм	100%	70 дБ	100%
25	-41 дБм	90%	60 дБ	100%
20	-52 дБм	80%	43 дБ	90%
21	-52 дБм	80%	40 дБ	80%
15	-63 дБм	60%	33 дБ	50%
10	-75 дБм	40%	25 дБ	35%
5	-89 дБм	10%	10 дБ	5%
0	-110 дБм	0%	0 дБ	0%

Стандарт 802.11-2020 определяет еще один параметр(метрику), называемую *качество сигнала* [*signal quality (SQ)*], который измеряет качество псевдошумовой кодовой корреляции, принимаемой радиомодулем. Простыми словами, качество сигнала может быть мерой того, что может влиять на способ кодирования (модуляции), которая связана со скоростью передачи.

Вы узнаете о методах кодирования в Главе 6. Все, что может увеличить частоту битовых ошибок [bit error rate(BER)], как например низкое SNR, может быть показано параметрами SQ. Информационные параметры и от RSSI и от SQ метрик могут передаваться с физического уровня PHY на подуровень MAC. Некоторые параметры SQ также могут быть использованы совместно с RSSI, как часть схемы оценки чистого канала [clear channel assessment (CCA)].



Хотя метрики SQ и RSSI технически разные измерения, большинство производителей Wi-Fi называет обе метрики одновременно просто как параметры RSSI. Для целей этой книги, всякий раз когда мы обращаемся к параметрам RSSI, мы имеем ввиду и параметры SQ и параметры RSSI.

Согласно стандарту 802.11-2020, RSSI - это мера принимаемой радиоволновой энергии. Сопоставление значений RSSI актуальной принимаемой мощности зависит от реализации. Другими словами, производители БЛВС могут определить параметры RSSI собственным способом. Актуальный диапазон значений RSSI от 0 до максимального значения (меньше или равно 255), которое каждый производитель может выбрать на свое усмотрение (называется *RSSI\_Max*). Многие производители публикуют свою реализацию RSSI в продуктовой документации и/или на своем вебсайте. Некоторые производители БЛВС не публикуют свои параметры RSSI. Из-за того, что реализация RSSI метрик является проприетарной, существует две проблемы при попытке сравнить значения RSSI между различными производителями беспроводных карт. Первая проблема это то, что производители могут выбрать два разных значения для RSSI\_Max. Производитель БЛВС А может выбрать шкалу от 0 до 100, в то время как производитель БЛВС Б может выбрать шкалу от 0 до 60. Из-за разницы в шкалах, Производитель БЛВС А будет показывать сигнал со значением RSSI 25, в то же время производитель Б будет показывать тот же сигнал с другим значением RSSI - 15. Также, радио карты, выпущенные производителем БЛВС А, используют большее количество значений RSSI, и, вероятно, являются более чувствительными при оценке качества сигнала и SNR(отношения сигнал-шум).

Вторая проблема с RSSI это то, что производители могут взять свой диапазон значений RSSI и сравнить их с другим диапазоном значений. Производитель БЛВС А может взять 100-значную шкалу и соотнести ее со значениями дБм от -110 дБм до -10 дБм, в то время как производитель БЛВС Б может взять свою 60-значную шкалу и соотнести ее со значениями дБМ от -95 дБм до -35 дБм. У нас не только разноисчисленные схемы, у нас также и различные диапазоны значений.

Хотя способ, которым производители Wi-Fi реализуют RSSI может быть проприетарным, большинство производителей похожи в том, что они используют пороги RSSI для критических механизмов, таких как роуминг и динамическое переключение скорости. Во время процесса роуминга, клиенты принимают решение о переходе с одной точки доступа на другую. Пороги RSSI являются ключевыми факторами для клиентов, когда они инициируют роуминговый переход. Пороги RSSI также используются производителями, чтобы реализовать *динамическое переключение скоростей* [*dynamic rate switching (DRS)*], которое является процессом, используемым

радиомодулями 802.11 для переключения между скоростями передачи данных. Роуминг обсуждается в нескольких главах этой книги, а DRS обсуждается более детально в Главе 13, “Концепции проектирования БЛВС.”

Так как сравнение RSSI между производителями может быть сложным из-за потенциального использования значений из разных численных шкал, многие программы сетевого мониторинга конвертируют значения RSSI в проценты, тем самым создавая общее сравнение.

Чтобы вычислить проценты RSSI, программное обеспечение сравнивает реальный сигнал со значением RSSI\_Max, которое является частью стандарта IEEE 802.11. Большинство производителей используют 0 в качестве базового значения для своих вычислений. Отсюда, нужно просто разделить RSSI принимаемого значения на RSSI\_Max, как показано на следующей формуле:

$$\text{RSSI/RSSI\_max} = \text{RSSI percentage}$$

Из предыдущего примера в этом разделе, производитель А имел шкалу от 0 до 100, и значение RSSI = 25, в тоже время производитель Б имел шкалу от 0 до 60, а RSSI = 15. В процентах RSSI будет одинаковый для обоих производителей: 25%.



## Пример из Реальной Жизни

### Может ли сетевая карта 802.11 достоверно измерить уровень шума?

Должно быть понятно, что ранние беспроводные сетевые интерфейсные карты 802.11 не являлись спектроанализаторами и, хотя они могли передавать и получать данные с невероятной скоростью, они не могли видеть необработанные окружающие радиосигналы. Так как через фильтр кодирования сетевой карты проходили только биты, вся информация, сообщаемая сетевой картой, должна была исходить из полученных битов. Если вы включили микроволновую печь около сетевой беспроводной карты, никаких битов данных не генерируется микроволновкой, таким образом, сетевая карта всегда будет сообщать, что переменная уровня шума равна нулю.

В отсутствие закодированных радиосигналов, приходящих от других устройств 802.11, переменная шума не может быть использована для определения уровня шума. Единственное устройство, которое могло действительно измерить незакодированную радиоволновую энергию, было *анализатор спектра*.

Мы знаем, что вы должно быть видели много экранов, показываемых вашими разными устройствами 802.11, которые отображали сигнал (переменная RSSI), и другое значение, отображаемое как отношение сигнал-шум (SNR), показывающее сравнение между RSSI и уровнем шума. Разработчики беспроводных сетевых карт знают, что радиолюбители «живут, дышат, и умирают» данными о сигнале, шуме и отношении сигнал-шум.

Профессионалы БЛВС просили реализовать отображение параметра шума, чтобы производить вычисления сигнала, поэтому различные организации производителей Wi-Fi пришли к тому, чтобы разными уникальными способами делать оценку уровня шума. Так как беспроводные сетевые карты 802.11 могли обрабатывать только биты, им нужно было придумать алгоритмы для вычисления переменной шума на основе битов, проходящих через сетевую карту.

Как и в случае измерений RSSI, различные производители оборудования 802.11 рассчитывали уровень шума по-разному. Некоторые производители наотрез отказались вычислять число для шума только на основе битов. Другие производители

разработали сложные алгоритмы для расчета шума.

Совсем недавно производители чипов стандарта 802.11 придумали, как отключить фильтры кодирования и использовать радиосигналы, проходящие через антенну, чтобы стать простейшим анализатором спектра. Однако, это вместо сетевой карты 802.11, способной обрабатывать данные. Обычно, эти новые чипы могут быть или простыми анализаторами спектра, или Wi-Fi картой, обрабатывающей данные, но обычно не одновременно в одно и тоже время, поскольку входной фильтр идентифицирует сигнал 802.11 и передает его в стек протоколов 802.11, а не на анализатор спектра. Некоторые точки доступа могут работать в, что иногда называется, «гибридном» режиме. Эти точки доступа могут выполнять функции и 802.11 и анализатора спектра одновременно, хотя часто с деградацией в производительности БЛВС. Дополнительно, некоторые производители БЛВС предлагают точки доступа со встроенным набором микросхем анализатора спектра, который работает независимо от радиомодуля Wi-Fi. Так какой же инструмент лучше всего подходит для точного измерения уровня шума в любой среде? Наиболее точным инструментом является откалиброванный анализатор спектра. Высококачественный портативный анализатор спектра использует набор микросхем анализатора спектра, способный измерять некодированную радиочастотную энергию, а его портативность делает его лучшим инструментом для измерения реального уровня шума. Имейте в виду, однако, что то, что анализатор спектра воспринимает как минимальный уровень шума, может отличаться от интерпретации минимального уровня шума радиомодулем 802.11 в клиенте БЛВС или точке доступа.

## Бюджет линии связи

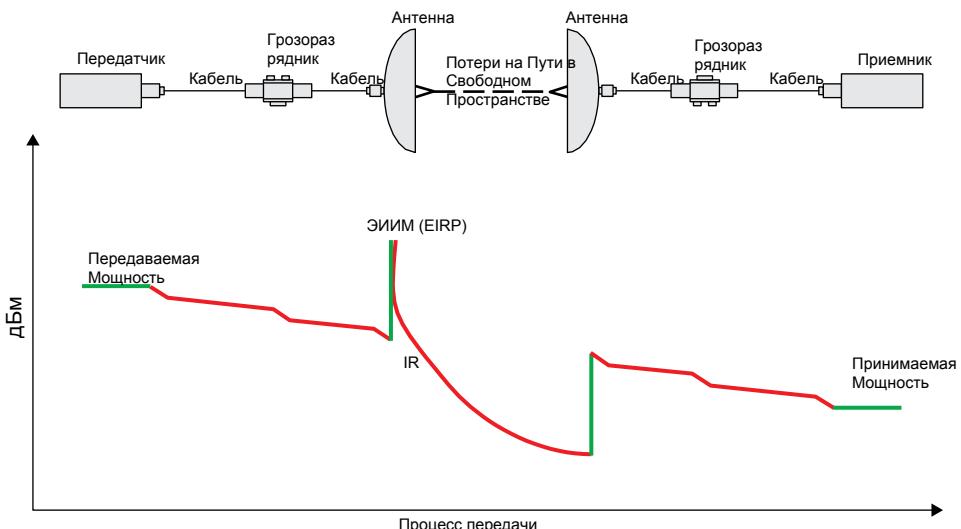
Когда развернута радиосвязь, бюджет линии связи - это сумма всех планируемых и ожидаемых усилений и потерь от передающего радиомодуля, через радио среду, к радиомодулю приемника. Назначение вычислений бюджета линии связи - гарантировать, что финальная амплитуда принимаемого сигнала выше порога приемной чувствительности радиомодуля приемника.

Расчеты бюджета канала включают исходное усиление передачи, усиление пассивной антенны и активное усиление радиочастотных усилителей. Все усиления должны быть учтены - включая усилители и антенны - и все потери должны быть учтены - включая аттенюаторы, потери на пути в свободном пространстве (FSPL), и вносимые потери. Любое физическое устройство, установленное в радиосистеме, добавляет некоторое количество потери сигнала, называемое *вносимые потери [insertion loss]*. Кабельные потери в dB рассчитываются на каждые 100 метров (или футов), соединители (коннекторы) обычно добавляют 0,5dB потерь.

Вы уже знаете, что радиоволны затухают по мере прохождения через свободное пространство. Рисунок 4.3 показывает беспроводной мост - канал связи точка-точка и показывает, что потери происходят по мере прохождения сигнала через различные радиокомпоненты, также как сигнал затухает из-за потерь на пути в свободном пространстве.

РИСУНОК 4.3

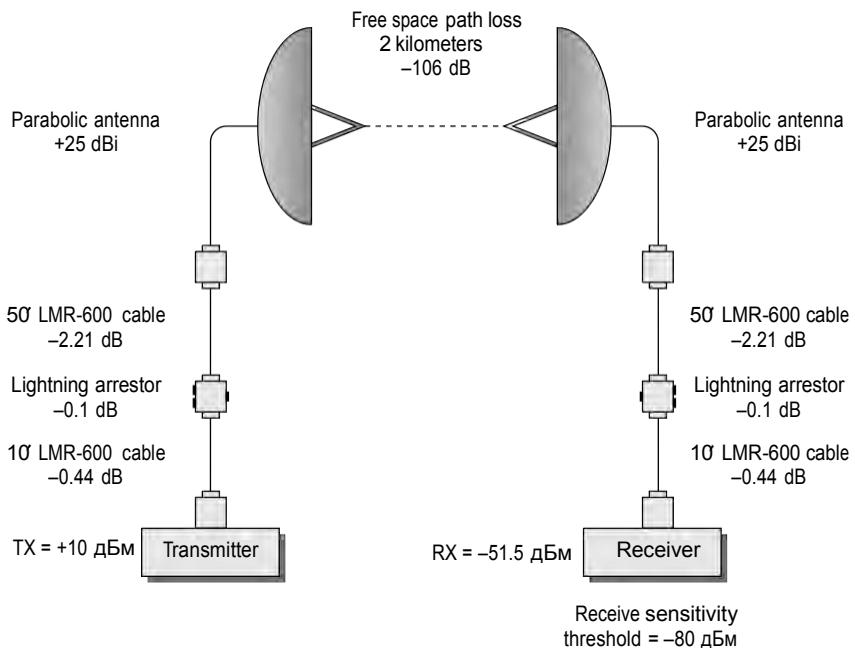
Компоненты бюджета линии связи



В верхней части рисунка находятся компоненты, которые образуют канал связи точка-точка, а нижняя часть рисунка представляет увеличение или уменьшение радиосигнала по мере продвижения сигнала от передатчика к приемнику. Передатчик начинает процесс создания сигнала определенной величины. Этот сигнал уменьшается пока движется к передающей антенне. Кабели, разъемы (соединители) и грозоразрядники - все уменьшают сигнал. Антenna фокусирует передаваемый сигнал, производя усиление, которое увеличивает сигнал. Самая большая потеря сигнала любой радиопередачи вызывается потерями на пути в свободном пространстве (FSPL) по мере путешествия сигнала к принимающей антенне. Эта antenna фокусирует принимаемый сигнал, производя усиление, увеличивая сигнал. Сигнал затем уменьшается снова так как он проходит через кабели, разъемы (соединители) и грозоразрядник, до тех пор, пока не дойдет до приемника. Этот рисунок является репрезентативным и выполнен не в масштабе.

Давайте рассмотрим вычисления бюджета линии связи беспроводного моста точка-точка в 2,4ГГц, как показано на Рисунке 4.4 и Таблицы 4.5 В нашем случае, две антенны в 2х километрах друг от друга, и исходной мощности передачи +10дБм. Обратите внимание на величину вносимых потерь, вызванных каждым радиочастотным компонентом, например кабелем и грозовыми разрядниками. Антенны пассивно усиливают сигнал, а сигнал ослабляется по мере прохождения через свободное пространство. Финальный принимаемый сигнал на приемном конце моста канала связи -51.5 дБм.

**Р И С У Н О К 4 . 4** Увеличение и уменьшение бюджета канала связи точка-точка



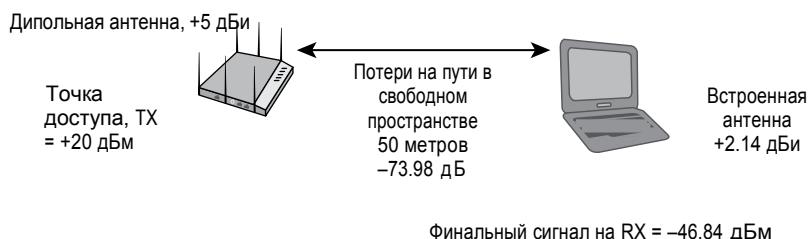
Давайте предположим, что порог приемной чувствительности радиомодуля приемника составляет  $-80$  дБм. Любой сигнал, получаемый с амплитудой выше  $-80$  дБм, может быть понят радиомодулем приемника, в то же время любая амплитуда ниже  $-80$  дБм не может быть понята. Вычисления бюджета линии связи определили, что финальный принимаемый сигнал равен  $-51.5$  дБм, что заметно выше порога приемной чувствительности  $-80$  дБм. Существует буфер  $28.5$  дБ между финальным принимаемым сигналом и порогом приемной чувствительности. Буфер  $28.5$ , который был определен во время вычислений бюджета линии связи называется, как *запас на замирания [fade margin]*, которые обсуждаются в следующем разделе.

Вы можете быть удивлены, почему эти числа отрицательные, когда до сих пор большинство дБм чисел, с которыми вы работали, были положительными. Рисунок 4.5 показывает простую сводку усилений и потерь в офисной среде. До сих пор вы работали в основном с расчетом IR и EIRP. Именно эффект потерь на пути в свободном пространстве (FSPL) делает значения отрицательными, как вы увидите в расчетах, основанных на Рисунке 4.5. В этом примере, принимаемый сигнал - это сумма всех компонентов:

$$+20 \text{ дБм} + 5 \text{ дБи} - 73.98 \text{ дБ} + 2.14 \text{ дБи} = -46.84 \text{ дБм}$$

**ТАБЛИЦА 4.5** Бюджет канала связи

Компонент	Усиление или затухание	Сила сигнала
Приемопередатчик (начальный сигнал передачи)		+10 дБм
10' LMR-600 кабель	-0.44 дБ	+9.56 дБм
Грозоразрядник	-0.1 дБ	+9.46 дБм
50' LMR-600 кабель	-2.21 дБ	+7.25 дБм
Параболическая антенна	+25 дБи	+32.25 дБм
Потери на пути в свободном пространстве	-106 дБ	-73.75 дБм
Параболическая антенна	+25 дБи	-48.75 дБм
50' LMR-600 кабель	-2.21 дБ	-50.96 дБм
Грозоразрядник	-0.1 дБ	-51.06 дБм
10' LMR-600 кабель	-0.44 дБ	-51.5 дБм
Приемник (финальный принимаемый сигнал)		-51.5 дБм

**РИСУНОК 4.5** Усиление и потери бюджета линии связи в офисе

Хотя изначальная амплитуда передачи будет почти всегда выше 0 дБм (1 мВт), амплитуда финального принимаемого сигнала будет всегда хорошо ниже 0 дБм (1 мВт) из-за потерь в свободном пространстве (FSPL).

## Запас на замирания/Операционный(Рабочий) запас системы

Запас на замирания (*Fade margin*) – это уровень желаемого сигнала выше чем того, что требуется. Хороший способ объяснить запас на замирание – это думать об этом как о зоне комфорта. Если приемник имеет приемную чувствительность -80 дБм, передача будет успешной до тех пор, пока принимаемы сигнал больше чем -80 дБм.

Проблема в том, что принимаемый сигнал флюктуирует из-за множества внешних влияний, таких как интерференция и погодные условия. Чтобы приспособиться к флюктуации, общепринятой практикой является планирование буфера от 10дБ до 25дБ выше порога чувствительности приема радио, используемого в канале связи типа мост. Буфер от 10дБ до 25дБ выше приемного порога чувствительности является запасом на замирание.

Пусть приемник имеет чувствительность  $-80$  дБм, а сигнал обычно принимается на  $-76$  дБм. При нормальных условиях, связь является успешной. Однако, из-за внешних влияний, сигнал может колебаться на  $\pm 10$ дБ. Это значит, что большую часть времени, связь является успешной, но в тех случаях когда сигнал отклоняется на  $-86$  дБм, связь будет не успешной. Добавляя запас на замирание 20дБ в вычисления бюджета линии связи, вы теперь говорите, что для ваших нужд, приемная чувствительность  $-60$  дБм, и вы будете планировать вашу сеть так, чтобы принимаемый сигнал был больше  $-60$  дБм. Если принимаемый сигнал флюктуирует, вы уже имеете встроенную некоторую подушку - в этом случае 20дБ.

Смотрите Рисунок 4.4. Если вам требуется запас на замирание 10дБ выше приемной чувствительности  $-80$  дБм, количество сигнала, требуемого для канала связи, будет  $-70$  дБм . Поскольку сигнал рассчитан на прием на уровне  $-51,5$  дБм, вы будете иметь успешную связь. Этот сигнал будет адекватным даже если вы выберете запас на замирание 20 дБ.

Поскольку на радиосвязь могут влиять многие внешние факторы, общепринято иметь запас на замирания, чтобы обеспечить уровень надежности канала связи. Увеличивая запас на замирания, вы существенно увеличиваете надежность канала связи. Думайте о запасе на замирания как о буфере или запасе на ошибки для принятых сигналов, которые используются при проектировании и планировании радиосистемы. После того как канал радиосвязи установлен, важно измерить канал, чтобы увидеть каков действительный размер буфера или подушки. Это функциональное измерение называется, как Операционный (Рабочий) Запас Системы (*system operating margin (SOM)*). Операционный запас системы - это разница между действительным принимаемым сигналом и сигналом, необходимом для надежной связи.



## Пример из Реальной Жизни

### Когда нужны вычисления запаса на замирания?

Когда бы не проектировался внешний БЛВС мостовой канал связи, расчет бюджета линии связи и запаса на замирание будет абсолютным требованием. Например, радиоинженер может выполнить расчеты бюджета линии связи для 2х-мильного мостового канала связи точка-точка и определить, что итоговый принимаемый сигнал на 5 дБ выше порога приемной чувствительности радиомодуля на одном конце мостового канала связи. Может показаться, что радиосвязь будет хорошей, однако, из-за замираний, вызванных многолучевым распространением и погодными условиями, требуется буфер запаса на замирания. Проливной ливень может ослабить сигнал на 0,08 дБ на милю (0,05 дБ на километр) в диапазонах частот 2,4 ГГц и 5 ГГц. На длинных мостовых каналах связи обычно рекомендуется запас на замирания 25дБ, чтобы компенсировать затухание вызванные изменениями поведения распространения радиоволн, таких как многолучевое распространение, и изменениями погодных условий, таких как дождь, туман или снег.

При развертывании Wi-Fi сети внутри помещения, где присутствуют условия высокого многолучевого распространения или высокий уровень шума, лучшая практика – это планирование запаса на замирание на примерно 5дБ больше от рекомендованной производителем амплитуды приемной чувствительности. Например, –70 дБм или более сильный сигнал попадает выше порога RSSI для высоких скоростей передачи данных для большинства производителей БЛВС радиомодулей. Во время радиообследования внутри помещений, показатель радиоизмерения в –70 дБм часто используется, чтобы определить область покрытия для высоких скоростей передачи данных. В зашумленной среде, показатель радиоизмерения в –65 дБм, использующие запас на замирания в 5 дБ, являются рекомендованной лучшей практикой.

## УПРАЖНЕНИЕ 4. 3

### Бюджет Линии Связи и Запас на Замирание

В этом упражнении вы будете использовать Microsoft Excel файл чтобы вычислить бюджет линии связи и запас на замирания. Вам понадобится Excel, установленный на вашем компьютере.

1. Загрузите файл LinkBudget.xls с онлайн ресурса книги ([www.wiley.com/go/cwnasg6e](http://www.wiley.com/go/cwnasg6e)) на рабочий стол, а затем откройте его.
2. В ряду 10, введите длину канала связи в **25** километров.  
Заметьте, что потери на пути из-за 25 километрового канала связи теперь составляют 128дБ на 2,4ГГц.
3. В ряду 20, введите **128** в дБ для потери в пути.
4. В ряду 23, измените чувствительность радио приема на **–80** дБм.  
Обратите внимание, что финальный принимаемый сигнал теперь –69 дБм и запас на замирания только 11 дБ.
5. Попробуйте увеличить выходную мощность радиопередатчика, чтобы увидеть, как будет работать соединение, и определить, какая мощность потребуется для обеспечения запаса на замирание в 20 дБ. Вы также можете изменить другие компоненты, такие как усиление антенны и кабельные потери, чтобы обеспечить запас на замирания в 20 дБ.

## Итого

Эта глава покрывает следующие шесть ключевых областей радиосвязи:

- Радиокомпоненты
- Радиоизмерения
- Радиоматематика
- Пороги RSSI
- Бюджеты линии связи

- Запасы на замирания

Важно понимать, как каждый радиокомпонент влияет на выход приемопередатчика. It is important to understand how each RF component affects the output of the transceiver. Всякий раз, когда компонент добавляется, удаляется или модифицируется, выход радио связи изменяется. Вам необходимо понимать эти изменения и быть уверенными, что система соответствует регуляторным стандартам. Следующие радиокомпоненты были рассмотрены в этой главе:

- Передатчик
- Приемник
- Антenna
- Изотропный излучатель
- Расчетный излучатель (IR)
- Эквивалентная Изотропно Излучаемая Мощность (ЭИИМ(EIRP))

В дополнение к пониманию компонентов и их влияния на передаваемый сигнал, вы должны знать различные единицы мощности и сравнения, которые используются, чтобы измерить выход и изменения радиосвязи:

- Единицы мощности
  - Ватт
  - Милливатт
  - дБм
- Единицы сравнения
  - дБ
  - дБи
  - дБд

После того как вы стали знакомы с радиокомпонентами и их влиянием на радиосвязь, и вы знаете различные единицы мощности и сравнения, вам необходимо понимать, как выполнить актуальные вычисления и определить будет ли ваша радиосвязь успешной. Вам необходимо понимать, как выполнять расчеты, а также некоторые термины и понятия, связанные с проверкой того, что канал радиосвязи будет работать правильно. Вот эти концепции и термины:

- Правило 10и и 3х
- Уровень шума
- Отношение Сигнал-Шум(SNR)
- Отношение Сигнал к Интерференции плюс Шум (SINR)
- Чувствительность приема
- Индикатор Силы Принимаемого Сигнала (RSSI)
- Бюджет Линии Связи
- Операционный запас системы (SOM)
- Запас на замирания

# Темы Экзамена

**Понимать радиокомпоненты.** Знать функцию каждого компонента, и какой компонент добавляет усиление, а какой компонент добавляет потери.

**Понимать единицы мощности и сравнения.** Убедитесь, что вы комфортно себя чувствуете, когда вас спрашивают про разницу между единицами мощности (абсолютными) и единицами сравнения (относительными). Знать все единицы мощности и сравнения, что они измеряют, и как они используются.

**Уметь выполнить простые радио математические действия.** Никаких логарифмов не тесте не будет; однако, вы должны знать как использовать правило 10и и 3х. Вам нужно уметь рассчитать результат на основе сценария, значений мощности, или относительных изменений.

**Понимать практическое использование радио математики.** Когда все сказано и сделано, главный вопрос заключается в том, будет ли работать радиосвязь? Именно здесь критически важно понимание RSSI, SOM, запаса на замирание и бюджета канала.

**Уметь объяснить важность измерения отношения сигнал-шум(SNR) и уровня шума.** Понимать, что окружающий фоновый уровень радиоэнергии на определенном канале может повредить передачу данных 802.11. Понимать, что единственное устройство, которое действительно может измерить немодулированную радио энергию - это анализатор спектра.

**Дать определение RSSI.** Понимать, что радиомодули используют метрики RSSI, чтобы интерпретировать силу сигнала и качество. Радиомодули 802.11 используют метрики RSSI для принятия решений таких, как роуминг и динамическое переключение скоростей.

**Понимать необходимость бюджета линии связи и запаса на замирание.** АБюджет линии связи - это сумма всех усилий и потерь от передающего радиомодуля, через радио среду, к приемному радиомодулю. Цель бюджета линии связи - гарантировать, что амплитуда финального принимаемого сигнала выше порога приемной чувствительности приемного радиомодуля. Запас на замирания - это уровень полезного сигнала выше требуемого.

## Проверочные Вопросы

1. Что из перечисленного является более лучшим показателем того, что внешние воздействия влияют на радиосигнал в определенный момент времени?

  - A. RSSI
  - B. SNR
  - C. EIRP
  - D. SINR
  
2. Точечный источник, который излучает радиосигнал одинаково во всех направлениях называется как ?

  - A. Всенаправленный генератор сигналов
  - B. Всенаправленная антенна
  - C. Расчетный излучатель
  - D. Ненаправленный передатчик
  - E. Изотропный излучатель
  
3. При вычислении бюджета линии связи и операционного запаса системы для внешнего БЛВС мостового канала связи точка-точка, какие факторы стоит взять во внимание? (Выберите все что применимо.)

  - A. Расстояние
  - B. Приемная чувствительность
  - C. Амплитуда передачи
  - D. Высота антенны
  - E. Кабельные потери
  - F. Частота
  
4. Сумма всех компонентов от передатчика до антennы, не включая антенну, называется как? (Выберите два.)

  - A. IR
  - B. Изотропный излучатель
  - C. ЭИИМ(EIRP)
  - D. Рсчетный излучатель
  
5. Какой термин используется, чтобы описать количество радиоэнергии от головы антennы?

  - A. Эквивалентная изотропная излучаемая мощность
  - B. Излучаемая мощность передающей антенной
  - C. Общая излучаемая мощность
  - D. Антеннная излучаемая мощность

- 6.** Выберите абсолютные единицы мощности. (Выберите все что применимо.)
- A.** Ватт  
**B.** Милливатт  
**C.** Децибел  
**D.** дБм  
**E.** Бел
- 7.** Выберите единицы сравнения (относительные). (Выберите все что применимо.)
- A.** дБм  
**B.** дБи  
**C.** Децибел  
**D.** дБд  
**E.** Бел
- 8.** 2 дБд равен скольким дБи?
- A.** 5 дБи  
**B.** 4.41 дБи  
**C.** 4.14 дБи  
**D.** 2 дБи
- 9.** 23 дБм равен скольким мВт?
- A.** 200 мВт  
**B.** 14 мВт  
**C.** 20 мВт  
**D.** 23 мВт  
**E.** 400 мВт
- 10.** Беспроводной мост настроен на передачу 100 мВт. Антенный кабель и разъемы дают 3дБ потерь, и подключены к антенне 16дБи. Какой ЭИИМ(EIRP)?
- A.** 20 мВт  
**B.** 30 дБм  
**C.** 2,000 мВт  
**D.** 36 дБм  
**E.** 8 Вт
- 11.** Передатчик БЛВС, который излучает сигнал 400мВт, подключен к кабелю с потерями в 9дБ. Если кабель подключен к антенне с 19дБи усиления, то каков будет ЭИИМ(EIRP)?
- A.** 4 Вт  
**B.** 3,000 мВт  
**C.** 3,500 мВт  
**D.** 2 Вт

- 12.** Производители БЛВС используют пороги RSSI, чтобы переключать какую характеристики радио карты? (Выберите все что применимо.)
- A.** Приемная чувствительность
  - B.** Роуминг
  - C.** Повторные передачи
  - D.** Динамическое переключение скоростей передачи данных
- 13.** Метрики Индикатора силы принимаемого сигнала(RSSI) используются радиомодулями 802.11, чтобы определить какие радио параметры?
- A.** Сила сигнала
  - B.** Фаза
  - C.** Частота
  - D.** Модуляция
- 14.** дБи является мерой чего?
- A.** Выход передатчика
  - B.** Увеличение сигнала, вызванного антенной
  - C.** Увеличение сигнала расчетного передатчика
  - D.** Сравнение между изотропным излучателем и приемопередатчиком
  - E.** Сила расчетного излучателя
- 15.** Что из перечисленного ниже является корректными вычислениями, при использовании правила 10-и и 3-х? (Выберите все что применимо.)
- A.** На каждые 3 дБ усиления (относительного), удваивается абсолютная мощность(мВт).
  - B.** На каждые 10dB потерь (относительных), делить абсолютную мощность (мВт) на 2.
  - C.** На каждые 10dB потерь (абсолютных), делить относительную мощность (мВт) на 3.
  - D.** На каждые 10мВт потерь (относительных), умножать абсолютную мощность (дБ) на 10.
  - E.** На каждые 10dB потерь (относительных), уполовинивать абсолютную мощность (мВт).
  - F.** На каждые 10dB потерь (относительных), делить абсолютную мощность (мВт) на 10.
- 16.** БЛВС передатчик, который излучает 100мВт сигнал, подключен кабелем с 3дБ потерями. Если кабель был подключен к антенне с 7дБи усилением, како будет ЭИИМ(EIRP) на антенном элементе?
- A.** 200 мВт
  - B.** 250 мВт
  - C.** 300 мВт
  - D.** 400 мВт

- 17.** В нормальной беспроводной мостовой сети, самые большие потери сигнала вызваны каким компонентом канала связи?
- A.** Приемная чувствительность
  - B.** Потери в антенном кабеле
  - C.** Грозоразрядник
  - D.** Потери на пути в свободном пространстве
- 18.** Чтобы удвоить эффективную дистанцию сигнала на определенном уровне мощности, насколько дБ должен быть увеличен ЭИИМ (EIRP)?
- A.** 3 дБ
  - B.** 6 дБ
  - C.** 10 дБ
  - D.** 20 дБ
- 19.** Во время радиообследования канала связи точка-точка между зданиями на производственном заводе, инженер БЛВС определил, что уровень шума чрезвычайно высок из-за всех машин, которые работают в зданиях. Инженер обеспокоен окружающим шумом из зданий, влияющий на внешний мостовой канал связи. Какая рекомендуемая лучшая практика имеет дело с этим сценарием?
- A.** Увеличить амплитуду передачи точки доступа БЛВС моста на 5-10 дБ.
  - B.** Установить точку доступа БЛВС моста выше.
  - C.** Удвоить расстояние сигнала точки доступа БЛВС моста с 6дБи антенным усилением.
  - D.** Запланировать для принимаемой амплитуды запас на замирания 5-10дБ.
- 20.** Какая величина не должна использоваться для сравнения беспроводных сетевых радиомодулей, произведенных различными производителями БЛВС?
- A.** Максимальная скорость передачи данных
  - B.** Максимальная мощность передачи
  - C.** Усиление антенны
  - D.** Индикатор Силы Принимаемого Сигнала



# Глава **5**

A black and white photograph of a lighthouse situated on a rocky coastline. The lighthouse is white with a dark lantern room and is surrounded by several buildings, possibly keeper's houses. The foreground consists of large, light-colored rocks. The ocean waves are visible in the background under a cloudy sky.

# Радиосигнал и Основы Теории Антенн

---

**В ЭТОЙ ГЛАВЕ, ВЫ УЗНАЕТЕ О СЛЕДУЮЩЕМ:**

- ✓ Графики диаграммы направленности по Азимуту и по Углу Места (огибающая излучения антенны)
- ✓ Интерпретация полярных диаграмм
- ✓ Ширина луча
- ✓ Типы антенн
  - Всенаправленные антенны
  - Всенаправленные антенны с уклоном вниз
  - Полунаправленные антенны
  - Узконаправленные антенны
  - Секторные антенны
  - Антенные решетки
- ✓ Линия прямой видимости
- ✓ Радиоволновая линия прямой видимости
- ✓ Зоны Френеля
- ✓ Изгиб(Выпуклость) Земли
- ✓ Антennaя поляризация
- ✓ Антенное разнесение
- ✓ Много вводов, много выводов (MIMO)
  - Антенные MIMO



#### ✓ Установка и соединение антенн

- Коэффициент Стоячей Волны по Напряжению (VSWR)
- Потеря сигнала
- Крепление антенны

#### ✓ Антенные аксессуары

- Кабели
- Разъемы
- Делители
- Усилители
- Аттенюаторы
- Грозоразрядники (молниезащита)
- Заземляющие стержни и провода

#### ✓ Соответствие нормативным требованиям



Чтобы иметь возможность связи между двумя или более приемопередатчиками, радиочастотный (РЧ) сигнал должен излучаться антенной передатчика с достаточной мощностью,

чтобы он был принят и понят приемником. Установка антенн имеет самую большую способность повлиять на то, будет ли связь успешной. Установка антенн может быть настолько простой, как размещение точки доступа в середине небольшого офиса, чтобы обеспечить полное покрытие вашей компании, или она может быть настолько сложной, как установка набора направленных антенн, что-то вроде сборки пазлов. Не бойтесь этот процесс, при правильном понимании антенн и того как они работают, вы можете обнаружить, что успешное планирование установки антенн в беспроводной сети является искусственной и вознаграждаемой задачей.

Эта глава фокусируется на категориях и типах антенн и различных способах, которыми они могут направлять радиосигнал. Выбор и установка антенн – это как выбор и установка освещения в доме. Во время установки домашнего освещения, у вас большой выбор: настольные лампы, потолочное освещение, направленные споты с узким и широким лучом. Глава 4, «Компоненты, Параметры и Математика Радиосвязи», познакомила вас с концепцией антенн, фокусирующих радиосигнал. В этой главе вы узнаете о различных типах антенн, их диаграмм направленностей, и то, как использовать различные антенны в различных средах.

Вы также узнаете, что хотя мы часто используем свет для объяснения излучения радиоволн, но существуют различия в том как они ведут себя. Вы узнаете о нацеливании и выравнивании или юстировке антенн, узнаете, что то, что вы видите не обязательно то , что вы получите.

В дополнение к информации об антennaх, вы узнаете об аксессуарах, которые могут понадобиться для правильной установки антennы. В офисной среде вам может просто понадобится подключить антенну к точке доступа. При наружной установке вам понадобится специальный кабель и разъемы, грозозащита, и специальные монтажные кронштейны. Мы познакомим вас с компонентами, необходимыми для успешной установки антennы.

Итого: Вы получите знания, которые позволят вам правильно выбирать, устанавливать и настраивать(выравнивать) антennы. Эти навыки помогут вам успешно развернуть беспроводную сеть, будь то сеть точка-точка между двумя зданиями или сеть, обеспечивающая беспроводное покрытие всего университетского городка.

# Диаграммы направленности по Азимуту и по Углу Места (Огибающая излучения антенны)

Существует много типов антенн, спроектированных для множества разных целей, также как существует много типов приборов освещения, разработанных для множества разных целей. При покупке приборов освещения домой, это просто сравнить две лампы, включая их и рассматривая как каждая из них рассеивает свет. К сожалению, невозможно таким же способом сравнить антенны.

Реальное одновременное сравнение антенн требует, чтобы вы ходили вокруг антенн с радиоизмерительным устройством, производили многочисленные измерения сигнала, а затем нанесли измерения либо на землю, либо на кусок бумаги, чтобы отобразить окружающую среду. Несмотря на тот факт, что это времяёмкая задача, результаты могут быть искажены из-за внешних воздействий на радиосигнал, таких как мебель или другие радиосигналы в этом месте. Чтобы помочь потенциальным покупателям с их решением о покупке, производители антенн для своих антенн создают *азимутальные графики [azimuth charts]* и *графики по углу места [elevation charts]*, которые называются как диаграммы направленности. Эти диаграммы направленности создаются в контролируемой среде, где результаты не могут быть искажены внешними воздействиями, и представляют собой диаграмму направленности сигнала, излучаемого конкретной моделью антенны. Эти диаграммы также называют как *диаграммы в полярной системе координат [polar chart]* или *огибающая антенного излучения [antenna radiation envelopes]*.

В дополнение к антенным полярным диаграммам, существует большое количество компаний, которые предлагают программное обеспечение, которое позволяет вам произвести предиктивное проектирование беспроводной сети. Этот тип программного обеспечения использует диаграммы направленности антенн в сочетании со свойствами структур зданий по затуханию радиоволн, чтобы создать план проектируемого беспроводного покрытия.

Рисунок 5.1 показывает графики по азимуту и по углу места всенаправленной антенны. Азимутальный график, обозначенный "H-Plane" (это плоскость колебаний вектора магнитного поля), представляет собой вид сверху-вниз на диаграмму направленности антенны. Так как это всенаправленная антенна, то вы можете видеть из азимутального графика, что диаграмма направленности - это почти идеальный круг.

График по углу места, обозначенный "E-Plane" (это плоскость колебаний вектора электрического поля), показывает вид с боку диаграммы направленности антенны. Не существует стандартов, которые требовали бы, чтобы производители антенн выравнивали градусные отметки диаграммы с направлением, на которое смотрит антenna, поэтому, к сожалению, это является зоной ответственности читателя диаграммы понять ее и интерпретировать.

Вот несколько пунктов, которые помогут вам интерпретировать диаграммы направленности:

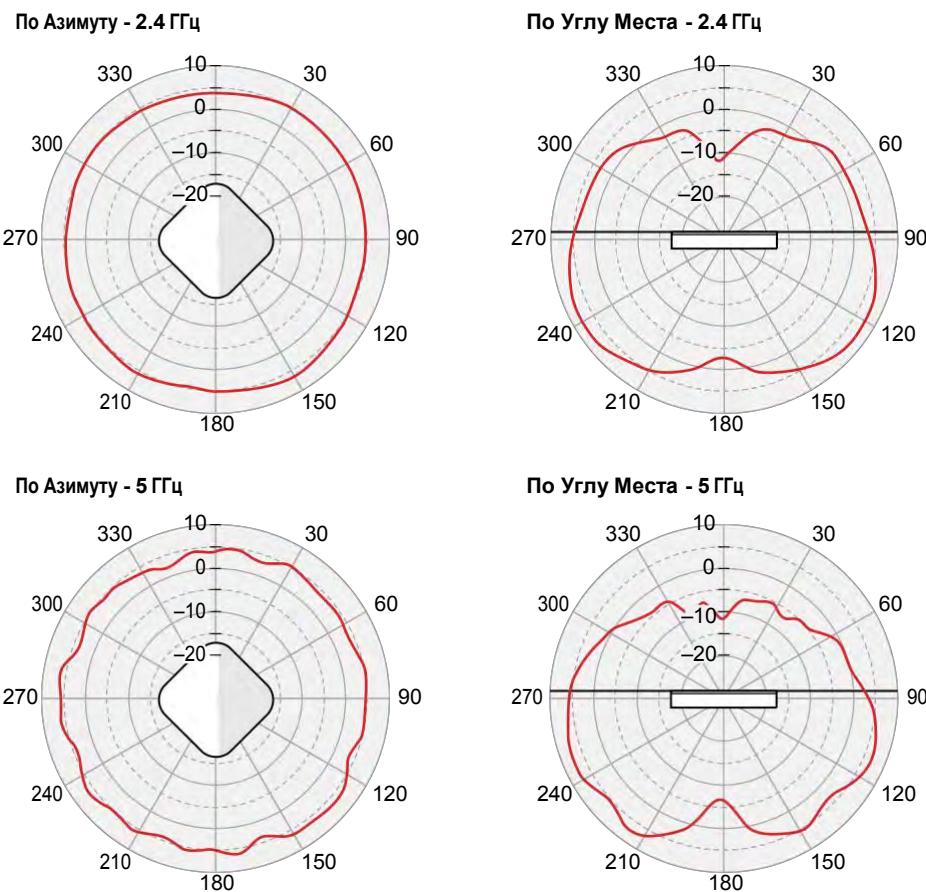
- На обоих диаграммах, антенна расположена в центре диаграммы.
- Азимутальная диаграмма = H-plane = вид сверху вниз

- Вертикальная диаграмма = E-plane = вид сбоку

Внешний круг диаграммы обычно представляет самый сильный сигнал антенны. Диаграмма не отражает расстояние или какой бы то ни было уровень мощности или силы, она отражает только отношение мощности между различными точками на диаграмме.

### Р И С У Н О К 5.1

### Диаграммы по Азимуту и Углу Места



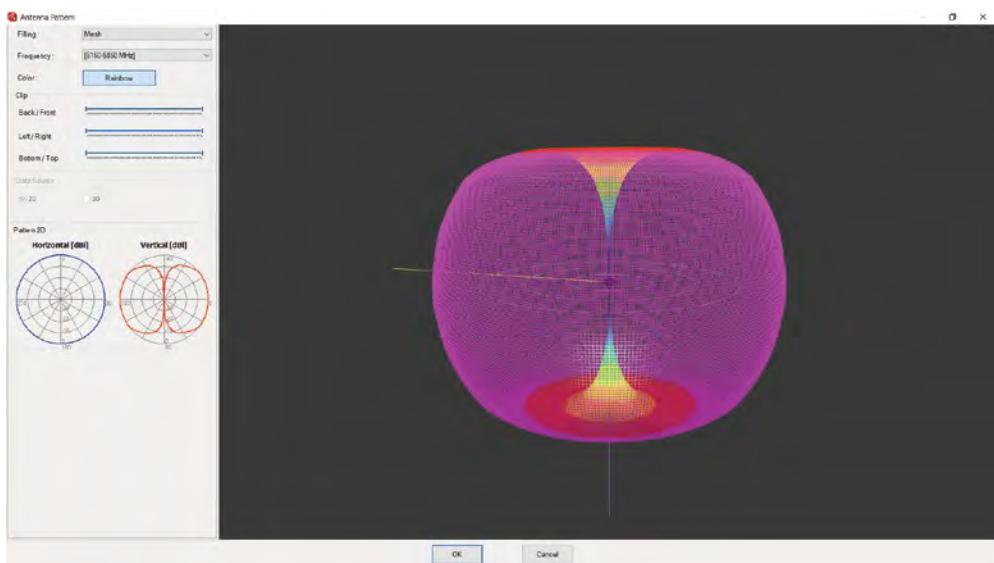
Один из способов представлять себе диаграмму это рассматривать ее так же как ведет себя тень. Если вы подносите фонарик ближе или дальше от своей руки, то тень от вашей ладони будет становиться больше или меньше. Тень не отображает размер руки. Тень дает представление об относительной форме руки. Будет ли тень больше или меньше, форма и вид тени руки будут идентичны. Для антенн диаграмма направленности будет больше или меньше в зависимости от того какую мощность получает антenna, но форма и соотношения, представленные диаграммой, всегда будут оставаться такими же.

Рисунок 5.2 показывает представление другой всенаправленной антенны. Этот график был получен с помощью предиктивного решения по моделированию от iBwave ([www.ibwave.com](http://www.ibwave.com)). На левой стороне графика даны представления антенны в H-плоскости (H-plane) и E-плоскости (E-plane). Основное изображение показывает 3хмерную сетчатую визуализацию покрытия антенны.

**РИСУНОК 5.2**

Представлено iBwave

Всенаправленная антенна: 3-мерный вид



## Трактовка Графиков в Полярных Системах Координат

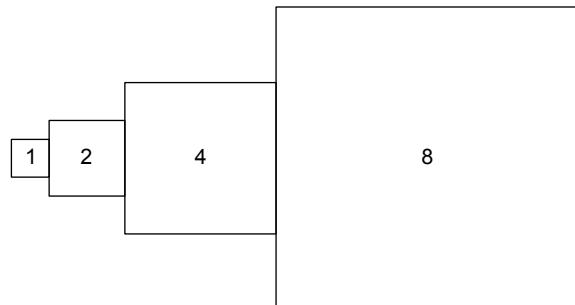
Как уже ранее упоминалось, диаграммы антенны по Азимуту(H-plane) и по Углу Места (E-plane), называются диаграммами в полярных координатах (или полярные диаграммы). Эти диаграммы часто неправильно трактуются и неправильно читаются. Одна из самых больших причин, по которой они неправильно трактуются, это то что они представляют отображение покрытия антенны в децибелах (дБ). Это отображение дБ представляет собой диаграмму направленности антенны; однако, она использует логарифмическую шкалу вместо линейной. Помните, что логарифмическая шкала - это переменная шкала, основанная на экспоненциальных величинах, таким образом полярные графики в действительности являются визуальным представлением, использующим переменную шкалу.

Взгляните на Рисунок 5.3. Числа внутри четырех блоков в верхнем левом углу говорят вам длину и ширину каждого блока. И хотя, визуально на нашей картинке мы представили блоки одинакового размера, в действительности каждый из них вдвое длиннее и шире чем предыдущий. Это легко нарисовать четыре блока одинакового физического размера и просто поставить число в каждом блоке, чтобы обозначить реальный размер блока. В середине рисунка мы нарисовали блоки, показывающие относительные размеры четырех блоков.

А что, если у нас больше блоков, скажем 10? Представляя каждый блок с помощью рисунка того же размера, легко изобразить блоки, как показано на рисунке в нижнем левом углу. В этом примере, если мы попытались бы показать реальную разницу в размерах, как мы это делали в середине рисунка, мы бы не смогли уместить рисунок на странице в книге. По факту, в комнате, в которой вы находитесь, может даже не хватить пространства чтобы ее нарисовать. Поскольку масштаб изменяется так резко, то не нужно рисовать блоки в масштабе, чтобы мы могли по прежнему представлять информацию.

**Р И С У Н О К 5 . 3**      Логарифмическое/линейное сравнение

1	2	4	8
---	---	---	---



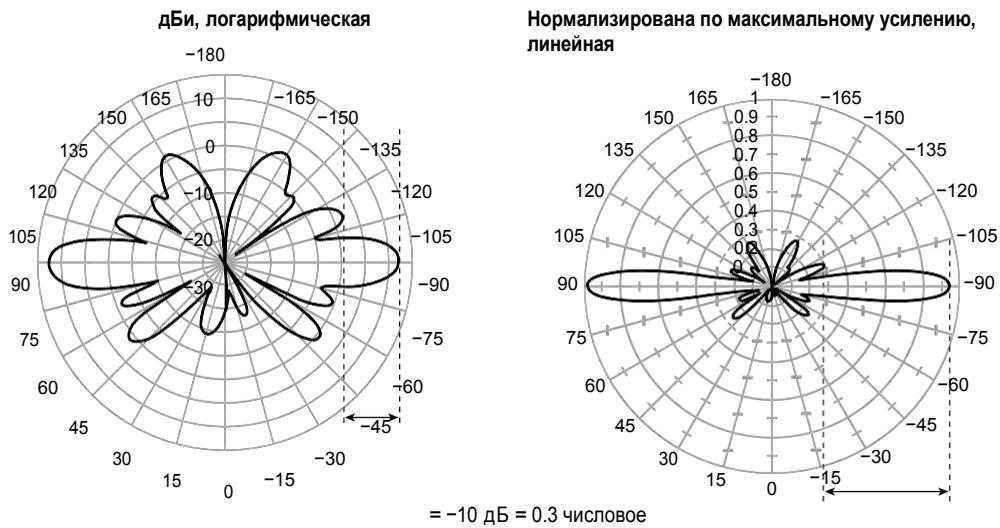
1	2	4	8	16	32	64	128	256	512
---	---	---	---	----	----	----	-----	-----	-----

Из Главы 4, вы узнали о радиоволновой математике. Одно из правил, которое вы узнали, было правило 6 дБ, которое гласит, что уменьшение на 6дБ мощности уменьшает фактическое расстояние, которое проходит радиосигнал, вдвое. Уменьшение на 10дБ по мощности уменьшает фактическое расстояние, которое проходит сигнал, примерно на 70 процентов. На Рисунке 5.4, левая полярная диаграмма показывает логарифмическое представление диаграммы по углу места всенаправленной антенны. Это как раз то, что вы обычно видите в брошюре об антенне или листочке с техническими характеристиками. Тот, кто не подготовлен к чтению таких диаграмм, вероятно взглянет на диаграмму и будет впечатлен тем насколько большое вертикальное покрытие обеспечивает антенна, но будет вероятно разочарован реальным покрытием.

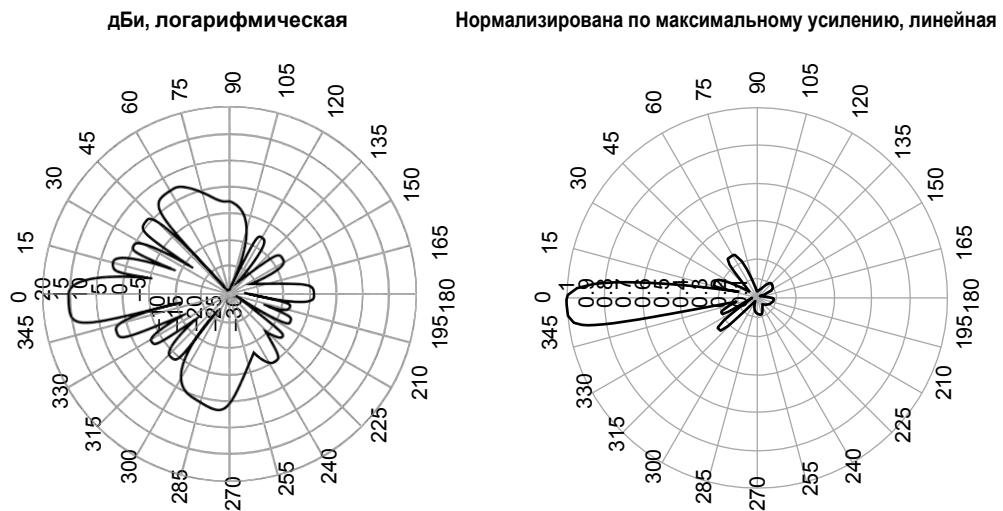
Читая логарифмическую диаграмму, вы должны помнить, что при уменьшении на каждые 10дБ от пикового сигнала, реальное расстояние уменьшается на 70 процентов. Каждый концентрический круг на этой логарифмической диаграмме представляет изменение в 5дБ. Рисунок 5.4 показывает логарифмический график диаграммы по углу места всенаправленной антенны вместе с линейным представлением ее покрытия. Обратите внимание, что первый боковой лепесток примерно на 10 дБ слабее основного лепестка. Не забудьте сравнить, где лепестки находятся относительно концентрических кругов. Это уменьшение на 10 дБ на логарифмической диаграмме равно 70-процентному уменьшению диапазона на линейной диаграмме. Сравнивая обе диаграммы, вы видите, что боковые лепестки на логарифмической диаграмме практически несущественны при переносе на линейную диаграмму. Как видите, эта всенаправленная антенна имеет очень маленькое покрытие по вертикали.

Еще одно сравнение, Рисунок 5.5 показывает логарифмический график диаграммы по углу места направленной антенны вместе с линейным представлением вертикального покрытия территории этой антенны. Мы повернули полярную диаграмму на бок, чтобы вы могли лучше видеть антенну, установленную на стене здания и направленную на другое здание.

**Р И С У Н О К 5 . 4**      Всенаправленная полярная диаграмма (Плоскость Е (E-plane))  
Изображение © Aruba Networks, Inc. Все права защищены. Используется с разрешения.



**Р И С У Н О К 5 . 5**      Направленная полярная диаграмма (Плоскость Е (E-plane))  
Изображение © Aruba Networks, Inc. Все права защищены. Используется с разрешения.

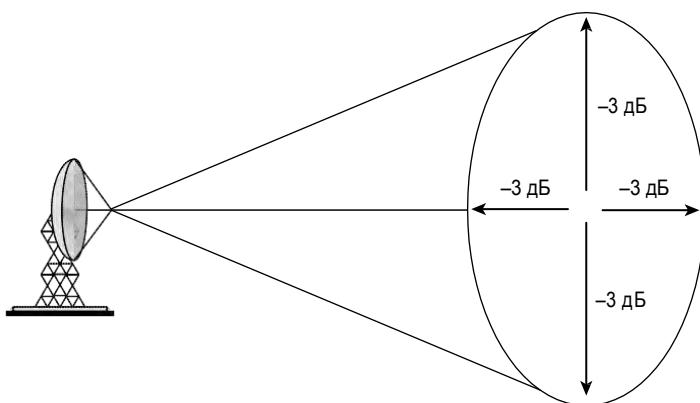


# Ширина луча

Многие фонарики имеют регулируемые линзы, позволяющие пользователю расширить или сузить концентрацию света. Радиоантенны способны фокусировать мощность, которая излучается от них, но в отличие от фонариков, антенны нерегулируемы. Пользователь должен решить сколько хотелось бы фокусировать прежде, чем приобрести antennу.

*Ширина луча [Beamwidth]* это мера того насколько широк или узок фокус антенны - и измеряется и по горизонтали и по вертикали. Измеряется от центра, или самой сильной точки сигнала антенны до каждой точки по горизонтальной и вертикальной осям, где сигнал уменьшается по мощности вдвое (-3дБ), как показано на Рисунке 5.6. Эти -3дБ точки часто называются точками половинной мощности. Расстояние между двумя точками половинной мощности на горизонтальной оси измеряется в градусах, давая значение ширины луча по горизонтали. Расстояние между точками половинной мощности по вертикальной оси также измеряется в градусах, и дает значение ширины луча по вертикали.

**Р И С У Н О К 5 . 6** Ширина луча антенны



Большую часть времени, пока вы решаете какая антenna будет решать ваши потребности в связи , вы будете рассматривать страницы с техническими характеристиками от производителей , чтобы определить технические характеристики антенны. Производители обычно указывают числовые значения ширины луча антенны по горизонтали и вертикали. Важно понимать как эти цифры вычисляются. Рисунок 5.7 иллюстрирует этот процесс.

## 1. Определение шкалы полярной диаграммы.

На этой диаграмме, внешняя сплошная линия представляет пиковый уровень сигнала. Двигаясь в центр круга, следующая сплошная линия это - на 10дБ меньше от пикового уровня сигнала, следующая ближе к середине - на 20дБ меньше от уровня пикового сигнала, и последняя сплошная линия - на 30 дБ меньше чем уровень пикового сигнала. Двигаясь в середину круга, пунктирная линия представляет -5дБ, -15дБ и -25дБ меньше чем пиковый уровень сигнала.

- 2.** Чтобы определить ширину луча антенны, найдите точку на диаграмме, где сигнал антенны самый сильный.

На этом примере, самый сильный сигнал , там куда указывает стрелка с номером 1.

- 3.** Двигайтесь вдоль графика антенны от пикового сигнала (как показано двумя стрелками с цифрами 2) пока не достигнете точки, где график антенны на 3dB ближе к центру диаграммы (как показано двумя стрелками с цифрами 3).

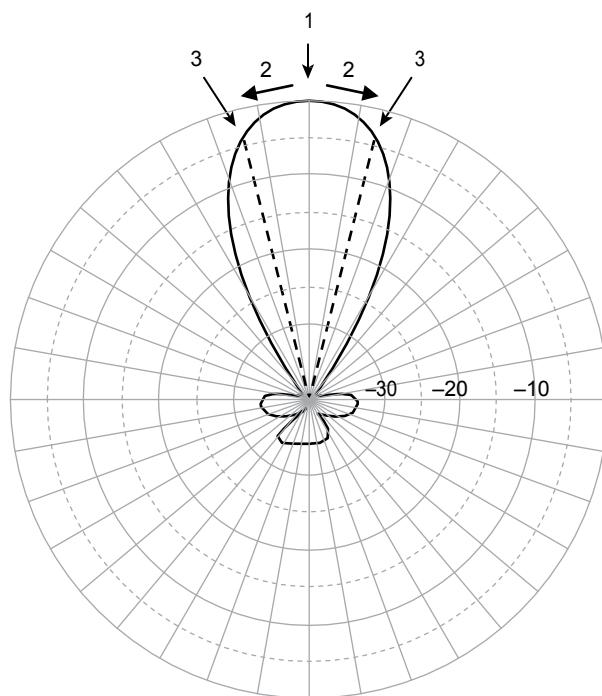
Вот зачем вам нужно сначала узнать шкалу диаграммы.

- 4.** Проведите линию от каждой из этих точек в середину полярной диаграммы (как показано темными пунктирными линиями).
- 5.** Измерьте расстояние в градусах между этими линиями, чтобы вычислить ширину луча антенны.

На этом примере, ширина луча антенны примерно 28 градусов.

### Р И С У Н О К 5 . 7

### Вычисление ширины луча



Важно понимать, что даже несмотря на то, что большая часть генерируемого радиосигнала сфокусирована в пределах ширины луча антенны, значительная часть сигнала все же может излучаться за пределами ширины луча, от так называемых боковых или задних лепестков антенны. Когда вы посмотрите на азимутальные диаграммы различных антенн, вы заметите, что некоторые из этих боковых и задних лепестков весьма значительны.

Хотя сигналы этих лепестков значительно меньше, чем сигнал основной ширины луча, они зависимы, и в определенных установках, очень функциональны. Когда вы настраиваете антенны точка-точка, важно, чтобы вы убедились, что вы действительно настроились на основной лепесток, а не на боковой лепесток.

Таблица 5.1 показывает типы антенн, используемых для связи по стандарту 802.11.



Таблица 5.1 предоставляет справочную информацию, которая будет полезна при знакомстве с различными типами антенн в этой главе.

**ТАБЛИЦА 5.1** Ширина луча антенны

Тип Антennы	Горизонтальная ширина луча (в градусах)	Вертикальная ширина луча (в градусах)
Всенаправленная	360	от 7 до 80
Панельная	от 30 до 180	от 6 до 90
Яги/Волновой канал	от 30 до 78	от 14 до 64
Секторная	от 60 до 180	от 7 до 17
Парabolicкая тарелка	от 4 до 25	от 4 до 21

## Типы Антенн

Существует три основных категории антенн:

**Всенаправленная** *Всенаправленные антенны* излучают радиосигнал способом аналогичным тому как настольная или напольная лампа излучает свет. Они спроектированы, чтобы обеспечить общее покрытие по горизонтали во всех направлениях.

**Полунаправленная** *Полунаправленные антенны* излучают радиосигнал способом аналогичным тому, как излучает свет настенный бра от стены или способом как уличные фонари светят вниз на улицу или парковку, обеспечивая направленный свет по большой территории.

**Узконаправленная** *Узконаправленные антенны* излучают радиосигнал в манере аналогичной тому как излучает прожектор или спот фокусирует свет на флаге или знаке.

Каждый тип антенны разработан с учетом различных целей.



Важно помнить что данный раздел обсуждает типы антенн, а не освещение. Хотя это и полезно обращаться к освещению, чтобы проводить аналогию с антеннами, но, критично помнить, что в отличие от освещения, радиосигналы могут проходить через твердые предметы, такие как стены и полы.

В дополнение к тому, что антенны, действующие как излучатели и фокусирующие сигналы, которые они передают, они еще фокусируют сигналы, которые они получают. Если вы когда-нибудь гуляли и смотрели на звезды, они могли показаться достаточно тусклыми. Если бы вы посмотрели на те же звезды в бинокль, они оказались бы ярче. Если бы вы использовали телескоп, они оказались бы еще ярче.

Антенны работают таким же способом. Они не только усиливают передаваемый сигнал, они также усиливают принимаемый сигнал. Микрофоны с высоким усилением работают точно так же, позволяя вам не только смотреть за действием вашего любимого спорта по телевидению, но также и слышать это действие.

### Как по Английски "Антенны": *Antennas* или *Antennae*?

Хотя это не имеет критического значения, многим людям часто интересно как будет множественное число на английском от слова антенна (*antenna*): *antennas* или *antennae*. Простой ответ - оба, но полный ответ - в зависимости от контекста. Когда антенна(*antenna*) используется как биологический термин (по-русски - это усики), множественное число будет *antennae*, например: *the antennae of a bug* - усики (антеннки) жука. Когда используется электронный термин, множественное значение обычно *antennas* (антенны), например: *the antennas on an access point* - антенны на точке доступа. Нужно заметить, что это не всегда так, и вы можете встретить, что в одних регионах использую *antennas*, а в других *antennae*. За дополнительной информацией, обращайтесь по адресу [grammarist.com/usage/antennae-antennas](http://grammarist.com/usage/antennae-antennas).

## Всенаправленные Антенны

Всенаправленная антенна излучает радиосигнал во все направления. Небольшая, в резиновой оболочке *дипольная антенна* [*rubber-coated dipole antenna*], иногда называемая в англоговорящих странах как *антенна-резиновый утенок* [*rubber duck antenna*], является классическим примером всенаправленной антенны и является типовой заводской антенной множества точек доступа, хотя большинство антенн теперь в пластиковом корпусе, а не резиновом. Идеальная всенаправленная антенна будет излучать радиосигнал одинаково во все направления, как теоретический изотропный излучатель, который обсуждался в Главе 4. Ближайшая вещь к изотропному излучателю -это всенаправленная дипольная антенна.

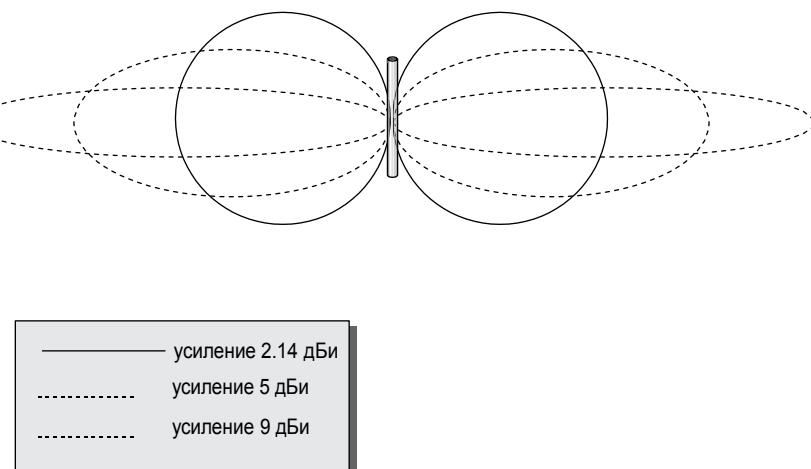
Простой способ объяснить диаграмму направленности всенаправленной антенны - это поднять и держать указательный палец вверх (он будет представлять антенну) и одеть на него бублик, как если бы это было кольцо (он представляет радиосигнал). Если вы разрежете бублик пополам горизонтально, как если бы вы собирались намазать на него масло, срезанная поверхность бублика будет представлять азимутальную диаграмму, или Н-плоскость (H-plane), всенаправленной антенны. Если вы возьмете другой бублик и

разрежете его вертикально, фактически разрезав отверстие, через которое вы смотрите, пополам, поверхность разреза бублика будет теперь представлять вертикальную диаграмму, или Е-плоскость(E-plane), всенаправленной антенны.

Из Главы 4, вы узнали, что антенны могут фокусировать или направлять сигнал, который они передают. Важно знать, что чем выше значение дБи или дБд антенны, тем больше фокусируется сигнал. При обсуждении всенаправленных антенн, не является не обычным первый вопрос о том, как возможно сфокусировать сигнал, который излучается во все стороны. У всенаправленных антенн с высоким усилением вертикальный сигнал уменьшается, а горизонтальная мощность увеличивается.

Рисунок 5.8 показывает вертикальный вид трех теоретических антенн. Заметьте, что сигнал антенн с более высоким усилением является более продолговатым, или более сфокусированным по горизонтали. Горизонтальная ширина луча всенаправленной антенны всегда 360 градусов, а вертикальная ширина луча меняется от 7 до 80 градусов, в зависимости от конкретной антенны.

**Р И С У Н О К 5 . 8**      Вертикальная диаграмма направленности всенаправленных антенн

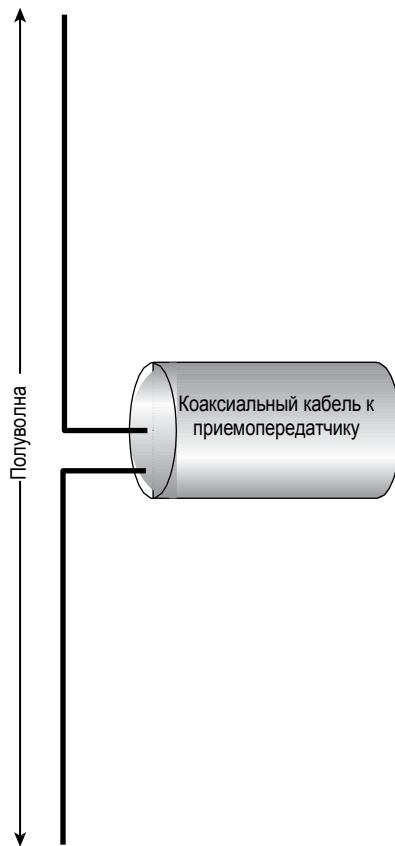


Из-за более узкого вертикального покрытия всенаправленных антенн с высоким усилением, важно тщательно планировать их использование. Размещая одну из таких антенн с высоким усилением на первом этаже здания можно обеспечить хорошее покрытие первого этажа, но из-за узкого вертикального покрытия, второй и третий этаж могут получить минимальный уровень сигнала. В некоторых случаях вы можете этого хотеть, в других нет. Внутренние установки обычно используют всенаправленные антенны с низким усилением, примерно 2.14 дБи.

Антенны наиболее эффективны, когда длина элемента составляет четную часть (например: 1/4 или 1/2) длины волны или кратна длине волны ( $\lambda$ ). Полуволновая 2.4 ГГц дипольная антенна (см Рисунок 5.9) состоит из двух элементов, каждый по 1/4 длины волны (около 1 дюйма), работающие в противоположных направлениях друг к другу. Всенаправленные антенны с более высоким усилением обычно построены путем установки друг на друга нескольких дипольных антенн и называемых *коллинеарные антенны* [ *collinear antennas* ].

**Р И С У Н О К 5 . 9**

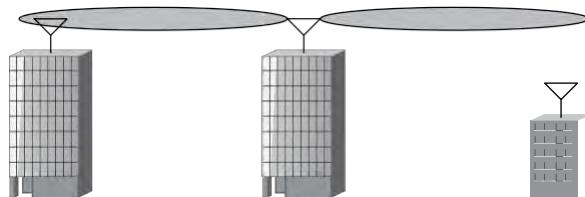
Полуволновая дипольная антенна



Всенаправленные антенны обычно используются в средах точка-многоточка. Всенаправленная антенна, подключенная к устройству (такому как точка доступа), которое располагается в центре группы клиентских устройств, предоставляет централизованные возможности связи окружающим клиентам. Всенаправленные антенны с высоким уровнем усиления также могут быть использованы снаружи, чтобы соединить несколько зданий вместе в конфигурации точки-многоточка. Центральное здание будет иметь всенаправленную антенну на крыше, а окружающие здания будут иметь направленные антенны нацеленные на центральное здание. В этой конфигурации важно убедиться, что усиление всенаправленной антенны достаточно высокое, чтобы обеспечить необходимое покрытие, но не очень высокое, чтобы вертикальная ширина луча не оказалась слишком узкой, чтобы обеспечить адекватный сигнал для окружающих зданий.

Рисунок 5.10 показывает установку, где усиление слишком высоко. Здание слева будет способно связываться, но здание справа вероятно будет испытывать проблемы. Чтобы решить проблему, показанную на рисунке 5.10, используются секторные массивы в конфигурации с наклоном вниз вместо всенаправленных антенн с высоким уровнем усиления. Секторные антенны обсуждаются позже в этой главе.

**Р И С У Н О К 5.10** Неправильно установленная всенаправленная антенна



## Всенаправленные Антенны с уклоном вниз

Большинство ранних точек доступа (802.11a/b/g) имеет две дипольные антенны, которые торчат из точки доступа. Идеальная ориентация для этих антенн для более лучшего радиосигнала - это или поднятые прямо вверх, или опущенные прямо вниз. В корпоративной среде эти точки доступа обычно монтировали на потолок с антеннами, выступающими вниз из точки доступа. Иногда ТД монтировали на стены. Много дипольных антенн имеют шарниры в том месте, где они крепятся к ТД, давая им возможность оставаться быть ориентированными вертикально.

Проблема с внешними подключаемыми антеннами в том, что они часто не правильно устанавливаются, или спустя время, антенны сдвигаются и становятся не вертикально ориентированными. Что может происходить из-за того, что человек, устанавливающий точку доступа и антенны не знает как правильно монтировать и выравнивать их, антенны будут установлены с разной ориентацией , чтобы они имели более эстетический вид, или из-за того, что люди, видящие антенны в качестве вызова для них чтобы допрыгнуть до них и достать их.

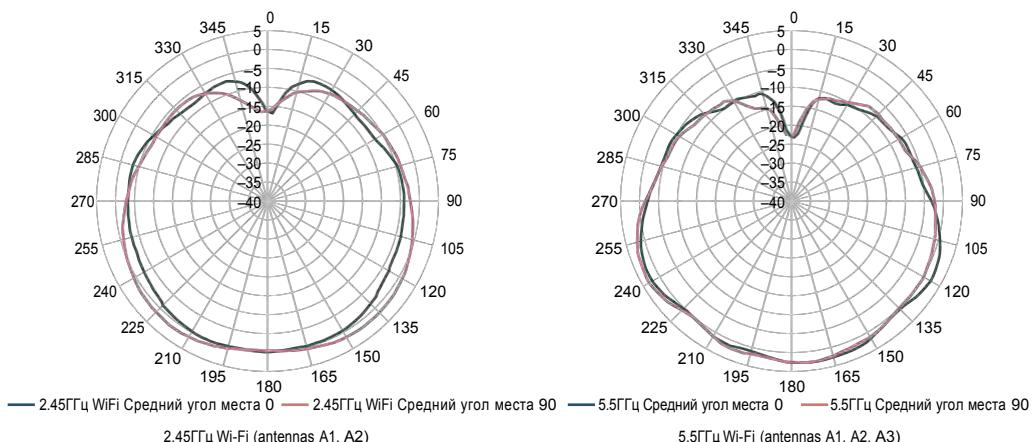
Другая проблема с установкой всенаправленных дипольных антенн около потолка это то, что эти антенны излучают радиосигнал выше и ниже антенн. При установке точек доступа и антенн на потолке, типовая задача - обеспечить услугами БЛВС тех, кто располагается на территории под точкой доступа, однако, большая часть радиосигнала теряется, излучаясь выше точки доступа.

С введением технологий MIMO в 802.11n, производительность БЛВС стала зависеть от ТД, использующих много антенн одновременно. С технологией MIMO, ориентация всех антенн точек доступа стала более критичной. Чтобы обеспечить более сфокусированный сигнал под точкой доступа, установленной на потолке, и обеспечить более лучшую связь MIMO, производители точек доступа разработали точки доступа со встроенными антennами, называемыми *всенаправленные антенны с уклоном вниз [downtilt omnidirectional antennas]*. Эти точки доступа спроектированы с массивом из множества антенн. Антенные элементы обычно располагаются так, чтобы обеспечить некоторое различие диаграммы направленности (различие в покрытии) между отдельными антеннами в массиве. Каждая антenna в массиве должна в основном покрывать туже самую область, однако, небольшое отличие между покрытиями антенн обеспечит слегка разные пути отражения для радиосигнала, что улучшает связь по технологии MIMO. Рисунок 5.1 показывает полярную диаграмму ТД со встроенными антеннами с уклоном вниз. Эта диаграмма показывает вертикальную диаграмму направленности в 2.4ГГц и 5ГГц точки доступа, повернутой на 0 градусов и на 90 градусов. Заметьте, что большее покрытие обеспечивается под ТД (центр диаграммы) и меньшее покрытие над ней.

### РИСУНОК 5.11 ТД с уклоном вниз и вертикальная диаграмма направленности

**Вертикальные плоскости (боковой вид, ТД смотрит вниз)**

Показан вид с боку с ТД, повернутой на 0 и 90 градусов



## Полунаправленные Антенны

В отличии от всенаправленных антенн, которые излучают радиосигнал во все направления, полунаправленные антенны спроектированы, чтобы направлять сигнал в определенном направлении. Полунаправленные антенны используются для связи на коротких и средних расстояниях, связь на больших расстояниях обслуживается узконаправленными антеннами.

Обычная практика использовать полунаправленные антенны для организации сетевого моста между двумя зданиями в кампусной среде или вдоль улицы друг за другом. Более длинные расстояния должны обслуживаться узконаправленными антennами.

Следующие три типа антенн попадают в категорию полунаправленных:

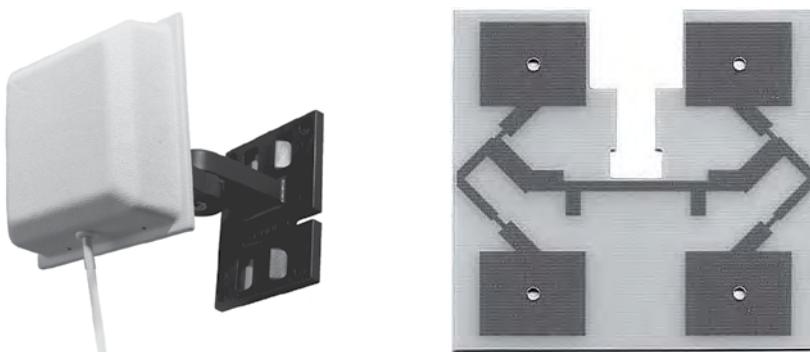
- Патч-антенны
- Панельные антенны
- Антенна Яги (или Антенна типа Волновой канал)

Патч-антенны и Панельные антенны, как показано на Рисунке 5.12, более точно классифицируются или называются как планарные антенны. Слово Патч(по англ. *Patch* - заплатка, лоскут) указывает на определенный способ дизайна излучающих элементов внутри антенны. К сожалению, стало общей практикой использовать термины *патч-антенна* и *панельная антенна* взаимозаменяемо. Если вы не уверены в конкретике дизайна антенны, лучше называть ее как *планарная антенна*.

Эти антенны могут быть использованы для наружной связи точка-точка на расстояние до одной мили (примерно 1,61 км), но наиболее обычно используются в качестве центрального устройства для обеспечения однонаправленного покрытия от точки доступа до клиентов во внутренних помещениях. Обычная практика для патч-антен и панельных антенн - это быть подключенными к точкам доступа для обеспечения направленного покрытия внутри здания. Планарные антенны могут быть эффективно использованы в библиотеках, складах и розничных магазинах с длинными рядами полок.

**Р И С У Н О К 5 .1 2**

Внешний вид патч-антенны и внутренний антенный элемент



Из-за высоких, длинных полок всенаправленные антенны имеют сложности с обеспечением эффективного радиопокрытия.

Наоборот, планарные антенны могут быть размещены высоко на боковых стенах здания, направляя их через ряды полок. Антенны можно чередовать между рядами, при этом каждая вторая антенна размещается на противоположной стене. Так как планарные антенны имеют горизонтальную ширину луча 180 градусов или чуть меньше, то за пределы здания излучается минимальное количество сигнала. При чередующемся размещении антенн и направлении их с противоположных сторон здания, более вероятно, что радиосигнал будет излучаться вдоль по рядам, обеспечивая необходимое покрытие.

До прихода радио-технологии 802.11 MIMO, патч-антенны и панельные антенны использовались внутри помещений с устаревшими радио-технологиями 802.11a/b/g, чтобы помочь уменьшить отражения и надеясь уменьшить негативный эффект многолучевого распространения [multipath]. Полунаправленные антенны для установки в помещениях часто устанавливались в средах с высоким многолучевым распространением, таких как склады или розничные магазины с большим количеством металлических шкафов или полок. С технологией MIMO, патч-антенны и панельные антенны больше не нужны, чтобы уменьшать многолучевое распространение, так как многолучевое распространение имеет положительный эффект для технологии MIMO.

Патч-антенны MIMO все еще используются внутри помещений, но совсем по другой причине. Наиболее обычное использование MIMO патч-антенны для помещений в случае установки в высоко плотной среде. Среда высокой плотности может быть описана как небольшая область, где существует большое количество клиентских Wi-Fi устройств. Примером может быть школьный спортзал или актовый зал, наполненный людьми, использующими много Wi-Fi радиоустройств. В сценарии с высокой плотностью всенаправленная антенна может быть не самым лучшим решением для покрытия. MIMO патч-антенны и панельные антенны часто установлены на потолке или стене и направлены вниз, чтобы обеспечить узкий "сектор" покрытия. Самое типовое использование MIMO патч-антенны для помещений - в средах высокой плотности. Обсуждение использования внутренних MIMO патч-антенны можно найти в Главе 13 "Концепции Проектирования БЛВС".

Антенны Яги-Уда, показаны на Рисунке 5.13, более известны как антенны Яги (или Волновой канал, в отечественной технической литературе). Они обычно используются для связи на коротких и средних расстояниях до 2 миль, хотя антенны Яги с высоким усилением могут быть использованы для больших расстояний.

Другое преимущество полуунаправленных антенн это то, что они могут быть установлены высоко на стене и наклонены вниз на область которую нужно покрыть. Этого нельзя сделать со всенаправленными антеннами, без направления сигнала с другой стороны антенны вверх. Поскольку единственный радиосигнал, который излучается сзади полуунаправленной антенны, является случайным, возможность направлять его по вертикали является дополнительным преимуществом.

**Р И С У Н О К 5.13** Внешняя антенна Яги и ее внутренний антенный элемент

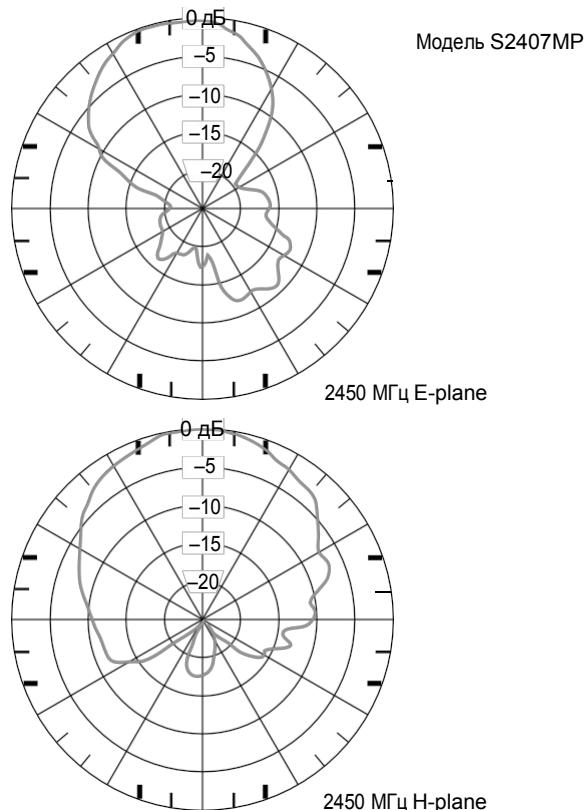


Рисунок 5.14 показывает диаграмму направленности типовой полуунаправленной панельной антенны. Помните, что эти реальные диаграммы направленности по азимуту и по углу места от определенной антенны, а у каждого производителя и модели антенны будут слегка другие диаграммы направленности.

## Узконаправленные Антенны

Узконаправленные антенны используются строго для связи точка-точка, обычно чтобы предоставить сетевой мост между двумя зданиями. Они обеспечивают наиболее сфокусированную, узкую ширину луча среди всех типов антенн.

**Р И С У Н О К 5.14** Диаграмма направленности типовой полуунаправленной антенны



Существует два типа узконаправленных антенн, *параболические тарелки* [*parabolic dish antennas*] и *решетчатые антенны* [*grid antennas*]:

**Параболические Антенны** Антенна типа параболической тарелки аналогична по виду небольшим цифровым спутниковым ТВ антеннам, которые можно увидеть на крыше многих домов.

**Решетчатые Антенны** Как показано на Рисунке 5.5, решетчатая антенна напоминает решетку гриля барбекю, с краями слегка загнутыми внутрь. Расстояние между проволокой в решетчатой антенне определяется длиной волны частот, для которых спроектирована антенна.

Благодаря высокому усилиению узконаправленных антенн, они идеальны для связи точка-точка на далекие расстояния.

Из-за длинных дистанций и узкой ширины луча, узконаправленные антенны больше подвержены влиянию антенной ветровой нагрузки, то есть движению или смещению антенны, вызванного ветром. Даже небольшое движение узконаправленной антенны может привести к тому, что луч радиосигнала будет направлен в сторону от приемной антенны, прерывая или ухудшая радиосвязь.

В условиях сильного ветра, решетчатые антенны, благодаря пространству между проволокой, менее восприимчивы к ветровой нагрузке и могут быть более лучшим выбором.

#### **Р И С У Н О К 5.15 Решетчатая антенна**

Изображение предоставлено Ventev ([www.ventevinfra.com](http://www.ventevinfra.com)).



Другой вариант в условиях сильного ветра - это выбор антенны с широким лучом. В этой ситуации, если антенна слегка сдвинется, сигнал будет продолжать приниматься из-за более широкой области покрытия. Помните, что чем шире луч, тем меньше усиление. Если используется сплошная тарелка, то категорически рекомендуется, использовать защитный кожух, который называется как обтекатель (англ. radome), чтобы помочь компенсировать некоторое воздействие ветра. Независимо от того, какой тип антенны установлен, качество крепления и антенны будут иметь огромное влияние на снижение ветровой нагрузки.

## **Секторные Антенны**

*Секторные антенны [sector antennas]* являются особым типом узконаправленных антенн с высоким усилением, полунаправленная антенна, которая даёт диаграмму направленности в виде куска пирога. Эти антенны обычно устанавливаются в середине области, где требуется радиопокрытие, и ставятся спиной к спине с другой секторной антенной. Отдельно, каждая антенна обслуживает свой собственный кусок пирога, но как группа, все куски пирога прижимаются друг к другу и обеспечивают всенаправленное покрытие для всей области. Совмещенные секторные антенны для обеспечения покрытия 360 градусов по горизонтали называются *массив секторов [sectorized array]*.

В отличие от других полунаправленных антенн, секторная антенна создает очень маленький радиосигнал позади антенны (*задний лепесток [back lobe]*) и следовательно не интерферирует с другой секторной антенной с которой работает.

Горизонтальная ширина луча секторной антенны от 60 до 180 градусов, с узкой вертикальной шириной луча от 7 до 17 градусов. Секторные антенны обычно имеют усиление не менее 10дБи.

Установка группы секторных антенн для обеспечения кругового покрытия дает много преимуществ по сравнению с установкой одной всенаправленной антенны:

- Начнем с того, что секторные антенны могут быть установлены высоко над землей и слегка наклонены вниз, с наклоном каждой антенны на угол, соответствующий покрытию территории. Всенаправленные антенны также могут быть установлены высоко над землей, однако, если всенаправленная антенна наклонена вниз одной стороной, то другая сторона направлена вверх.
- Так как каждая антенна покрывает отдельный участок, каждая антенна может быть подключена к отдельному приемопередатчику, и может передавать и принимать независимо от других антенн.

Это дает возможность для всех антенн передавать в одно и тоже время, обеспечивая значительно более высокую пропускную способность.

Единственная всенаправленная антенна способна передавать только одному устройству в единицу времени.

- Последнее преимущество секторных антенн над одной всенаправленной антенной это то, что усиление секторных антенн значительно больше усиления всенаправленной антенны, что дает значительно большее покрытие территории.

Секторные антенны активно используются для сотовой телефонной связи и редко используются в установках Wi-Fi. Секторные антенны иногда используются для Wi-Fi в качестве решения организации последней мили некоторыми Беспроводными Интернет Сервис Провайдерами (WISPs). Внешние секторные антенны эпизодически используются в установках на стадионах.



## Пример из Реальной Жизни

### Сотовые Секторные Антенны Повсюду

Когда вы идете или едете на машине по вашему городку или большому городу, обратите внимание на башни(или вышки) радиосвязи. На многих из этих башен есть то, что выглядит как кольца из антенн вокруг них. Эти кольца антенн являются секторными антеннами. Если башня имеет более одной группы или кольцо вокруг неё, то вероятно, несколько сотовых операторов используют одну и ту же вышку.

## Антенные Решетки

Антеннная решетка или Антенный массив [antenna array]- это группа из двух и более антенн, которые интегрированы вместе, чтобы обеспечить покрытие. Эти антенны часто работают вместе, чтобы осуществлять, что называется, *формирование луча* (*beamforming*, иногда так и называемое - *бимформинг*). Формирование луча - это метод концентрации радиоволновой энергии. Концентрация сигнала означает, что мощность сигнала будет больше, следовательно соотношение сигнал-шум (SNR) на приемнике будет также больше, обеспечивая более лучшую передачу.

Существует три разных типа формирования луча:

- Статическое формирование луча
- Динамическое формирование луча
- Формирование луча передачи

Следующие разделы объясняют каждый из этих типов формирования луча.

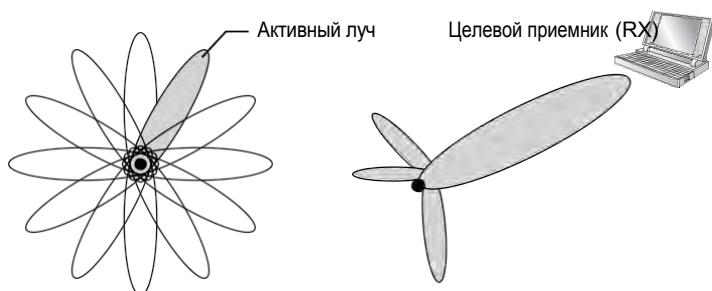
## Статическое формирование луча

*Статическое формирование луча* выполняется путем использования направленных антенн, чтобы обеспечить фиксированную диаграмму направленности. Статическое формирование луча использует несколько направленных антенн, сгруппированных вместе, но нацеленных в сторону от центральной точки или места. Статическое формирование луча это просто другой термин, иногда используемый, когда говорят о внутреннем массиве секторов. Хотя это уже не является обычным явлением, в прошлом один поставщик Wi-Fi производил решение для внутренней точки доступа с секторным массивом, в котором использовались направленные антенны для создания нескольких секторов луча.

## Динамическое формирование луча

*Динамическое формирование луча* фокусирует радиоволновую энергию в определенном направлении и в определенной форме. Также как статическое формирование луча, направление и форма сигнала являются сфокусированными. В отличие от статического формирования луча, диаграмма направленности сигнала может изменяться от кадра к кадру. Это может обеспечить оптимальную мощность и сигнал для каждой станции. Как показано на Рисунке 5.16, динамическое формирование луча использует *адаптивную антеннную решетку*, которая маневрирует лучом в направлении целевого приемника. Эта технология часто называется *технология умной(смарт) антенны*, или *управление лучом (beamsteering - бимстиринг)*. Возможность динамического формирования луча не доступна на клиентской стороне. Хотя это больше не является обычной практикой, в прошлом, некоторые производители Wi-Fi выпускали точки доступа, которые использовали собственные адаптивные антенные решетки.

**Р И С У Н О К 5.16** Динамическое формирование луча — адаптивная антенная решетка



Динамическое формирование луча может сфокусировать луч в направлении индивидуального клиента для нисходящей односторонней [unicast] передачи между

точкой доступа и целевым клиентом. Однако, любые широковещательные кадры, такие как маяк [beacon], передаются с использованием всенаправленной диаграммы так, чтобы точка доступа могла общаться со всеми близко находящимися клиентскими станциями во всех направлениях. Заметим, что хотя Рисунок 5.16 иллюстрирует концепцию, реальный луч вероятнее всего будет как диаграмма сигнала, созданного антенной, показанной на Рисунке 5.14.

## Формирование луча передачи

*Формирование луча передачи (TxBF)* производится путем передачи нескольких сигналов со смещением фазы с надеждой и целью того, что они прибудут с одинаковой фазой в место назначение, где, как полагает передатчик, находится приемник. В отличие от динамического формирования луча, TxBF не изменяет диаграмму направленности антенны, а реального направленного луча не существует. По правде, формирование луча передачи это не совсем антенная технология, это технология обработки цифровых сигналов на передающем устройстве, которая дублирует переданный сигнал на более чем одной антенне, чтобы оптимизировать комбинированный сигнал у клиента. Однако, аккуратное управление фазой передаваемых сигналов через несколько антенн имеет эффект улучшения усиления, таким образом эмулируя однонаправленную антенну с высоким усилением. Формирование луча передачи - это все про управление фазой передачи.

Поправка 802.11n определяет два типа формирования луча передачи: *неявное формирование луча передачи [implicit TxBF]* и *явное формирование луча передачи [explicit TxBF]*. Неявный TxBF использует неявный процесс анализа канала, чтобы оптимизировать разницу фаз между передающими цепями. Явный TxBF требует обратной связи от станции, для того чтобы определить величину фазового сдвига для каждого сигнала. Неявный TxBF так и не завоевал популярность на рынке; однако поддержка явного TxBF стала обычным явлением, начиная с поправки 802.11ac. Явный TxBF требует использования кадров измерения канала, и передатчик и приемник должны поддерживать формирование луча. Явный TxBF будет обсуждаться более детально в Главе 10, "Технология MIMO: НТ и VHT".

## Оптическая линия прямой видимости

Когда свет проходит от одной точки до другой, он проходит через то, что воспринимается как беспрепятственная прямая линия, называемая как видимая или оптическая линия прямой видимости [*line of sight (LOS)*]. Для всех задач и целей, это прямая линия, но из-за возможного светового преломления, дифракции, и отражения, есть небольшой шанс того, что это не так. Если вы были на улице летним днем и смотрели через раскаленную парковку на неподвижный объект, вы могли заметить, что из-за тепла, поднимающегося от тротуара, объект, на который вы смотрели, казался движущимся. Это пример того, как видимая линия прямой видимости (LOS) иногда слегка изменяется. Когда дело доходит до радиосвязи, видимая линия прямой видимости не влияет на успешность радиоволновой передачи.

# Радиоволновая линия прямой видимости

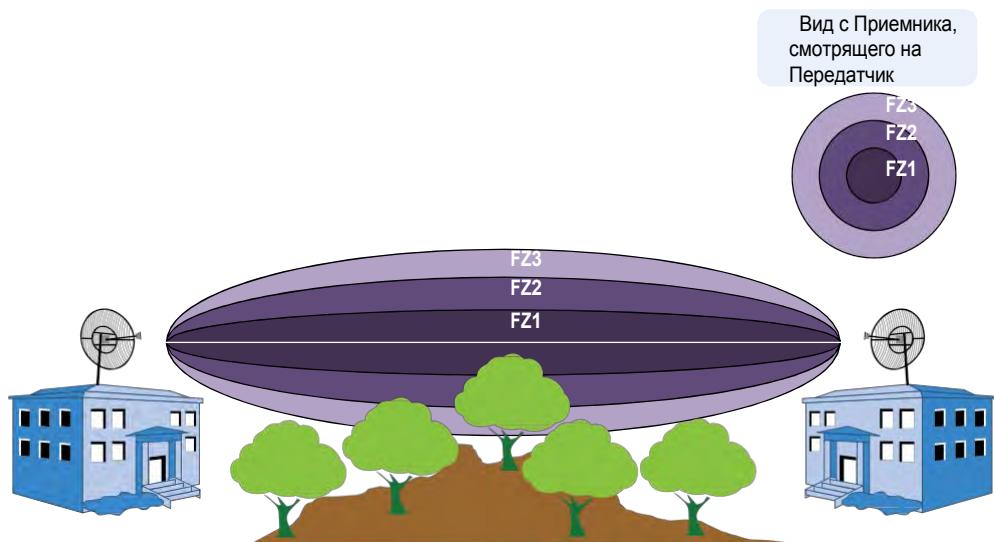
Радиосвязь точка-точка также нуждается в наличии беспрепятственной линии прямой видимости между двумя антеннами. Поэтому, первый шаг по установке системы точка-точка - это убедиться, что из точки установки одной антенны, у вас есть чистый прямой путь до другой антенны. К сожалению, чтобы радиосвязь работала корректно этого не достаточно.

Дополнительная область вокруг оптической линии прямой видимости должна оставаться чистой от препятствий и заграждений. Эта область вокруг оптической линии прямой видимости называется Зоной Френеля и часто называется *как радиоволновая линия прямой видимости [RF line of sight]*.

## Зона Френеля

Зона Френеля [*Fresnel zone*] - это воображаемая, продолговатая, в форме футбольного мяча (Американского футбола) область, которая окружает путь вдоль оптической линии прямой видимости между двумя антеннами точка-точка. Рисунок показывает иллюстрацию зоны Френеля в форме футбольного мяча.

**РИСУНОК 5.17**      Зона Френеля

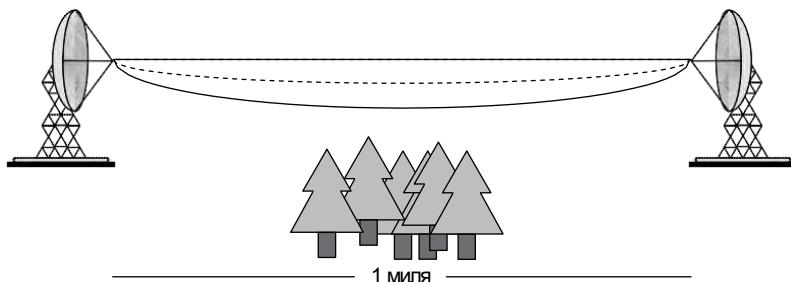


Теоретически, существует бесконечное число зон Френеля, или концентрических эллипсоидов (форма футбольного мяча), которые окружают оптическую линию прямой видимости. Ближайший эллипсоид называется первая зона Френеля, следующий - вторая зона Френеля, и т.д., как показано на Рисунке 5.17. Для простоты, только первые три зоны Френеля показаны на рисунке. Первые две имеют наиболее важное значение, а последующие зоны Френеля имеют небольшое влияние на связь.

Если первая зона Френеля становится даже частично загражденной, преграда будет негативно влиять на целостность радиосвязи. В дополнение к очевидному отражению и рассеянию, которое может произойти, если присутствует препятствие между двумя антеннами, радиосигнал может преломиться(испытать дифракцию), или изогнуться, по мере прохождения препятствия в зоне Френеля. Эта дифракция сигнала уменьшает количество радиоволновой энергии, которая принимается антенной, и может даже привести к обрыву канала связи.

Рисунок 5.18 иллюстрирует канал связи длиной в одну милю (примерно 1,61 км). Верхняя сплошная линия - это прямая линия от центра одной антенны до другой. Пунктирная линия показывает 60 процентов нижней половины первой зоны Френеля. Нижняя сплошная линия показывает нижнюю половину первой зоны Френеля. Деревья являются потенциальным препятствием на пути.

**РИСУНОК 5.18** Размер зоны Френеля 60 процентов и 100 процентов



Ни при каких обстоятельствах вы не должны разрешать ни какому объекту или объектам вторгаться более чем на 40 процентов в первую зону Френеля уличного канала связи типа мост точка-точка. Все что более 40 процентов, наиболее вероятно, сделает канал связи ненадежным. Даже препятствие менее 40 процентов, наверняка, ухудшит производительность канала связи. Следовательно, мы рекомендуем вам не допускать ни каких препятствий в первой зоне Френеля, особенно в лесных районах, где рост деревьев может загородить зону Френеля в будущем.

Типовые препятствия с которыми вы скорее всего сталкивались - это деревья и здания. Важно периодически воочию проверять ваш канал связи, чтобы удостовериться что деревья не проросли в зону Френеля, или что не построили здания, которые попали в зону Френеля. Не забывайте, что зона Френеля существует ниже, по бокам, и выше линии прямой видимости. Если зона Френеля стала загороженной, вам нужно или передвинуть антенну (обычно поднять ее) или удалить препятствие (обычно цепной пилой - шутка).

Чтобы определить будет ли препятствие попадать в зону Френеля, вам нужно знать несколько формул, которые позволят вам вычислить ее радиус. Не волнуйтесь, вас не будут тестировать на знание этих формул.

Первая формула позволит вам вычислить радиус первой зоны Френеля в средней точке между двумя антеннами. Эта точка, где зона Френеля имеет наибольший размер. Формула следующая:

$$\text{radius} = 72.2 \times \sqrt{[D \div (4 \times F)]}$$

radius = радиус в футах

D = расстояние канала связи в милях

F = частота передачи в ГГц

та же формула, но в метрах:

$$\text{radius} = 17.31 \times \sqrt{[D \div (4 \times F)]}$$

radius = радиус в метрах

D = расстояние канала связи в километрах

F = частота передачи в ГГц

Это оптимальный размер (зазор) который, должен быть вдоль линии сигнала. Хотя этот идеальный радиус не всегда возможен. Следовательно следующая формула будет очень полезна. Она может быть использована для вычисления радиуса зоны Френеля, которая позволит иметь вам 60 процентов от зоны Френеля незагороженной. Это минимальный размер чистого пространства, который вам нужен в средней точке между антеннами. Вот формула:

$$\text{radius (60\%)} = 43.3 \times [D \div (4 \times F)]$$

radius = радиус первой зоны Френеля в футах

D = расстояние канала связи в милях

F = частота передачи ГГц

та же формула, но в метрах:

$$\text{radius(60\%)} = 10.39 \times \sqrt{[D \div (4 \times F)]}$$

radius = радиус первой зоны Френеля в метрах

D = расстояние канала связи в километрах

F = частота передачи ГГц

Обе эти формулы полезны, но у них есть главный недостаток. Эти формулы вычисляют радиус зоны Френеля в средней точке между антеннами. Так как это точка, где зона Френеля имеет самый большой размер, это число можно использовать, чтобы определить необходимую высоту антенн, на которой они должны быть над землей. Вы должны знать это число, потому что если вы разместите антенну слишком низко, земля попадет в зону Френеля, и приведет к ухудшению связи. Проблема в том, что если есть известный объект где-то в отличном от средней точки месте между антеннами, то не возможно вычислить радиус зоны Френеля в этой точке используя эти уравнения. Следующая формула может быть использована для вычисления радиуса любой зоны Френеля в любой точке между двумя антennами:

$$\text{radius} = 72.2 \times \sqrt{[(N \times d1 \times d2) \div (F \times D)]}$$

radius = радиус зоны Френеля в футах

N = номер зоны Френеля, для которой производятся вычисления(обычно 1 или 2)

d1 = расстояние от одной антенны до места препятствия в милях

d2 = расстояние от препятствия до другой антенны в милях

D = общее расстояние между антеннами в милях (D = d1 + d2)

F = частота в ГГц

та же формула, но в метрах:

$$\text{radius} = 17.31 \times \sqrt{[(N \times d1 \times d2) \div (F \times D)]}$$

**radius** = радиус зоны Френеля в метрах

N = номер зоны Френеля, для которой производятся вычисления(обычно 1 или 2)

d1 = расстояние от одной антенны до места препятствия в километрах

d2 = расстояние от препятствия до другой антенны в километрах

D = общее расстояние между антеннами в милях (D = d1 + d2)

F = частота в ГГц

Рисунок 5.19 показывает канал связи точка-точка длиной 10 миль. Есть препятствие (дерево) в трех милях от одной антенны и 40 футов высотой. Итак, значения и формулы для вычисления радиуса зоны Френеля в точке 3 миль от антенны следующие:

N = 1 (для первой зоны Френеля)

d1 = 3 мили

d2 = 7 мили

D = 10 миль

F = 2.4 ГГц

$$\text{радиус на 3 миля radius} = 72.2 \times \sqrt{[(1 \times 3 \times 7) \div (2.4 \times 10)]}$$

$$\text{радиус на 3 миля} = 72.2 \times \sqrt{[21 \div 24]}$$

$$\text{радиус на 3 миля} = 67.53 \text{ фута}$$

Теперь посчитаем в метрах и километрах.

N = 1 (для первой зоны Френеля)

d1 = 3 километра

d2 = 7 километров

D = 10 километров

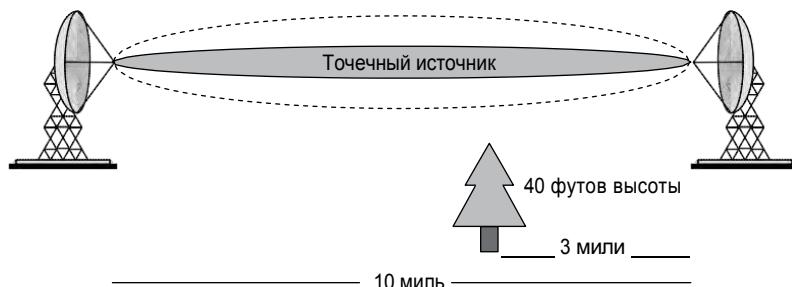
F = 2.4 ГГц

$$\text{радиус на 3 километре radius} = 17.31 \times \sqrt{[(1 \times 3 \times 7) \div (2.4 \times 10)]}$$

$$\text{радиус на 3 километре radius} = 17.31 \times \sqrt{[21 \div 24]}$$

$$\text{радиус на 3 километре radius} = 16.19 \text{ метров}$$

### Р И С У Н О К 5 .1 9      Связь точка-точка с потенциальным препятствием



Итак, если препятствие 40 футов (12,19 метра) в высоту, а зона Френеля в этой точке 67.53 фута (20,58 метра) высоты, то антенну нужно установить на высоте не менее 108 футов (32,92 метра) над землей, чтобы иметь достаточной чистую область (зазор, просвет или клиренс) ( $40' + 67.53' = 107.53'$ ; и округляем.) Если мы хотим позволить препятствию проникать на 40 процентов в зону Френеля, то нам нужно оставить свободными 60 процентов зоны Френеля. Итак, 60 процентов 67.53 фута (20,58 метра) это 40.52 фута(12,35 метра). Абсолютная минимальная высота антенны должна быть 81 фут (24,69 метра) ( $40' + 40.52' = 80.52'$ ; и снова округляем). В следующем разделе вы узнаете, что из-за выпуклости Земли, антенну нужно поднять еще выше, чтобы компенсировать земной изгиб.

При использовании узконаправленных антенн, ширина луча сигнала меньше, что приводит к тому, что будет передан более сфокусированный сигнал. Много людей считают, что меньшая ширина луча уменьшает размер зоны Френеля. Это не так. Размер зоны Френеля является функцией используемой частоты и расстояния канала связи. Так как единственны переменные в формуле это частота и расстояние, то размер зоны Френеля будет тем же самым независимо от типа антенны или ширины луча. Первая зона Френеля это технически область вокруг точечного источника, где волны находятся в фазе с точечным источником сигнала. Вторая зона Френеля тогда это область за первой зоной Френеля, где волны находятся не в фазе с точечным источником сигнала. Все нечетные номера зон Френеля находятся в фазе с точечным источником сигнала, а все четные номера зон Френеля находятся не в фазе.

Если радиосигнал одной и той же частоты, но находящийся не в фазе с главным сигналом, пересекает главный сигнал, то сигнал который не в фазе приведет к деградации или даже пропаданию основного сигнала. (Это было продемонстрировано в Главе 3 "Основы Радиотехники", упражнения с использованием веб приложения EMANIM). Один из способов, которым сигнал не в фазе может прервать основной сигнал - это отражение. Следовательно, важно рассмотреть вторую зону Френеля при оценке канала связи точка-точка. Если высота антенны и рельеф местности такой, что радиосигнал от второй зоны Френеля отражается в направлении приемной антенны, то может произойти ухудшение канала связи. Хоть это и не распространенное явление, вторую зону Френеля нужно принимать во внимание при планировании или поиске и устранении проблем канала связи, особенно на плоской, засушливой местности, как пустыня. Также нужно быть осторожным с металлическими поверхностями или водной гладью вдоль зоны Френеля.

Пожалуйста, поймите, что зона Френеля является трехмерной. Может ли что-нибудь быть помехой в зоне Френеля сверху? Хотя деревья не растут с неба, канал радиомоста точка-точка может проходить под железнодорожной эстакадой или скоростной автострадой. В этой редкой ситуации, следует уделить внимание правильному размеру свободного пространства для верхнего радиуса зоны Френеля. Более обычный сценарий развертывания каналов связи точка-точка в городской среде большого города. Очень часто каналы связи здание-здание должны проходит между другими зданиями. В этих ситуациях, другие здания потенциально могут перегородить боковой радиус зоны Френеля.

До сих пор, все обсуждения зоны Френеля касались связи точка-точка. Зона Френеля существует во всей радиосвязи, однако, именно во внешней связи точка-точка, она может вызвать множество проблем. Среда внутри помещений имеет так много стен и других препятствий, где уже существует так много отражений, преломлений, дифракций и рассеяний, что зона Френеля вряд ли влияет на успешность или обрыв канала связи.

# Выпуклость(Изгиб) Земли

Когда вы устанавливаете радиосвязь точка-точка на длинное расстояние, нужно принять во внимание еще одну переменную - это кривизна земли, также называемая как *изгиб(выпуклость) земли*. Так как ландшафт варьируется по всему миру, то невозможно определить точное расстояние, где кривизна земли будет влиять на канал связи. Рекомендация такова, что если антенны находятся друг от друга более семи миль (11,27 км), то вы должны учесть выпуклость(изгиб) земли, так как после семи миль (11,27км) земля сама начнет перекрывать зону Френеля. Следующую формулу можно использовать, чтобы вычислить дополнительную высоту, на которую нужно будет поднять antennу, чтобы компенсировать земную выпуклость (изгиб):

$$H = D^2 \div 8$$

H = высота земного изгиба в футах

D= расстояние между антеннами в милях

или

$$H = D^2 \times 0,08$$

H высота земного изгиба в метрах

D расстояние между антеннами в километрах

Теперь у вас есть все части, чтобы оценить на какой высоте нужно установить антенны. Помните, что это вычисляется оценка, так как она предполагает, что земля между антеннами не сильно варьируется по высоте. Вам нужно знать или подсчитать следующие три вещи:

- 60 процентов от радиуса первой зоны Френеля
- Высоту земной выпуклости (изгиба)
- Высоту любого препятствия, которое может попасть в зону Френеля, и расстояние до этого препятствия от антенны

Берем эти три части и складывая их вместе, получаем следующую формулу, которую можно использовать для вычисления высоты антенны:

$$H = \text{высота препятствия} + \text{земной изгиб} + \text{зона Френеля}$$

$$H = OB + (D^2 \div 8) + (43.3 \times \sqrt{D \div (4 \times F)})$$

$OB$  = высота препятствия

$D$  = расстояние канала связи в милях

$F$  = частота передачи в ГГц

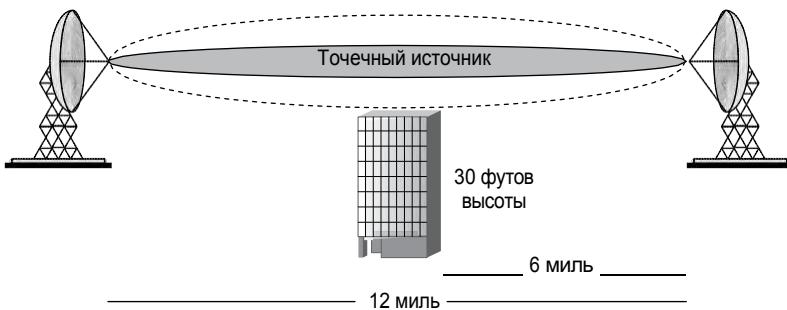
Рисунок 5.20 показывает канал связи точка-точка, который простирается на расстояние 12 миль. По середине этого канала находится офисное здание высотой 30 футов. Между двумя вышками используется сигнал 2.4 ГГц. Используя формулу, мы можем вычислить, что каждую антенну нужно будет установить на не менее чем 96,4 фута над землей.

$$H = 30 + (12^2 \div 8) + (43.3 \times \sqrt{[12 \div (4 \times 2.4)]})$$

$$H = 30 + 18 + 48.4$$

$$H = 96.4$$

**РИСУНОК 5.20** Расчет высоты установки антенны



Хотя эти формулы полезны, хорошая новость в том, что вам не нужно знать их для экзамена. Множество из этих формул также доступны в виде бесплатных онлайн калькуляторов. Один из таких ресурсов [www.everythingrf.com/rf-calculators](http://www.everythingrf.com/rf-calculators).

## Поляризация Антенны

Еще один момент, который нужно принять во внимание при установке антенн - это поляризация антенны. Хотя это менее известная проблема, она чрезвычайно важна для успешной коммуникации. Правильное выставление поляризации является критически важным при установке любого типа антенны. По мере излучения от

антенны, амплитуда волн может колебаться или вертикально или горизонтально. Важно, чтобы поляризация передающей и принимающей антенн были ориентированы одинаковым образом, чтобы получить самый мощный возможный сигнал. Установлены ли антенны с горизонтальной или вертикальной поляризацией обычно не важно, до тех пор пока обе антенны установлены с одной и той же поляризацией.



При обсуждении антенн, правильный термин - антенная *поляризация* [*polarization*], который обращается к положению или ориентации волн. Использование термина *полярность* [*polarity*] некорректно. Полярность указывает на положительное или отрицательное напряжение, которое не имеет отношение к ориентации антенны.

Поляризация не так важна для связи внутри помещений, так как поляризация радиосигнала часто меняется при отражении, что является обычным явлением в помещениях. Большинство точек доступа имеют встроенные антенны, или используют всенаправленные антенны с низким усилением, которые нужно устанавливать под потолком, имеют вертикальную поляризацию. Производители ноутбуков встраивают антенны по бокам от монитора. Когда экран ноутбука поднят, внутренние антенны также имеют вертикальную поляризацию.

Когда вы настраиваете радиомост точка-точка или точка-многоточка, правильная поляризация чрезвычайно важна. Если самый лучший уровень принимаемого сигнала (RSL), который вы получаете при настройке антенн, на 15 – 20 дБ меньше расчетного RSL, то велик шанс того, что у вас кросс-поляризация. Если же разница существует только с одной стороны, а у другой сигнал выше, то вы скорее всего навелись на боковой лепесток.



Прекрасное видео “Beam Patterns and Polarization of Directional Antennas,” («Виды Лучей и Поляризаций Направленных антенн») доступно для скачивания с онлайн ресурса книги, которое вы можете найти по адресу [www.wiley.com/go/cwnasg6e](http://www.wiley.com/go/cwnasg6e). Этот 3х минутный видеоролик объясняет и демонстрирует свойства боковых лепестков антенны и поляризации. Название файла видеоролика - *Antenna Properties.wmv*.

## Разнесение Антенн

Беспроводные сети, особенно внутренние сети, подвержены влиянию многолучевых [*multipath*] сигналов. При использовании не-ММО технологии (802.11a/b/g), чтобы помочь компенсировать влияние многолучевого распространения обычно используется разнесение антенн, также называемое как пространственное разнесение, в оборудовании беспроводных сетей., такого как точки доступа. *Разнесение антенн* [*Antenna diversity*] существует, когда точка доступа имеет две или более антенн с приемником, работающими вместе, чтобы минимизировать негативное влияние многолучевого распространения [*multipath*].

Так как длина волны беспроводных сетей 802.11 меньше 5 дюймов ( 12,7 см) в длину, антенны могут быть расположены очень близко друг к другу и позволять разнесению антенн быть эффективным. Когда точка доступа чувствует

радиосигнал, она сравнивает сигнал, который она получила на обеих антенных, и использует ту антенну, у которой выше сила сигнала, для приема кадра данных. Такая выборка выполняется от кадра к кадру, выбирая ту антенну, которая имеет более сильный сигнал.

Большинство пре-802.11n радиомодулей используют *переключаемое разнесение [switched diversity]*. Во время приема входящей передачи, переключаемое разнесение слушает несколько антенн. Много копий одного и того же сигнала поступает на приемные антенны с разными амплитудами. Выбирается сигнал с лучшей амплитудой, а остальные сигналы игнорируются. Точка доступа использует одну антенну до тех пор, пока сигнал выше предопределенного уровня сигнала. Если сигнал деградирует ниже приемлемого уровня, то точка доступа использует сигнал, принятый другой антенной.

Этот метод прослушивания на обнаружение лучшего принятого сигнала, также называется как *разнесение по приему [receive diversity]*. Переключаемое разнесение также используется при передаче, но используется только одна антenna.

Передатчик будет передавать через ту из разнесенных антенн, где сигнал с лучшей амплитудой был слышен последний раз. Метод передачи через антенну, где был последний раз слышен лучший принятый сигнал, также называется как *разнесение по передаче [transmit diversity]*.

Так как антенны так близко друг к другу, это не является необычным усомниться в том, что антенное разнесение действительно дает преимущества. Как вы помните из Главы 4, сила принятого радиосигнала часто меньше 0.0000001 милливатт. При таком уровне сигнала, легчайшая разница между сигналами, которые принимает каждая антenna, может быть колоссальной. Еще один фактор, о котором следует помнить, заключается в том, что точка доступа часто обменивается данными с несколькими клиентскими устройствами в разных местах. Эти клиенты не всегда стационарны, что в дальнейшем влияет на путь радиосигнала.

Точка доступа должна обращаться с передаваемыми данными по другому, нежели с принимаемыми. Когда точка доступа должна отправить данные обратно к клиенту, у нее нет способов определения с какой антенной клиент будет иметь лучший прием. Точка доступа может отправить передаваемые данные используя антенну, которая использовалась последний раз для приема данных. Запомните, что это часто называется *разнесением по передаче [transmit diversity]*. Не все точки доступа оснащены такой функциональностью.

Существует много видов разнесения антенн. У ноутбуков с внутренними картами обычно разнесенные антенны установлены внутри экрана ноутбука. Запомните, что из-за полудуплексной природы радиосреды, когда используется разнесение антенн, только одна антenna является рабочей в данное время. Другими словами, радио карта, передающая кадр с одной антеннами, не может принимать кадр с другой антеннами в одно и то же время.

## Много-Входов, Много-Выходов

*Много-входов, Много выходов [Multiple-input, multiple-output (MIMO)]* является другой более изысканной формой антенного разнесения. В отличие от обычных систем с одной передающей антенной, где многолучевое распространение является помехой, MIMO (произносится как МАЙ-мо) системы используют преимущество многолучевого распространения. MIMO можно смело назвать архитектурой беспроводной радиосвязи, которая принимает или передает используя много антенн одновременно. Сложные методы обработки сигналов позволяют значительно

улучшить надежность, дальность и пропускную способность в MIMO-системах. Эти методы посылают данные используя множество одновременных радиосигналов. Приемник затем реконструирует данные из этих сигналов.

С момента появления 802.11n, радиомодули БЛВС используют технологию MIMO. Одна из ключевых целей при установке MIMO устройств - удостовериться, что каждый из сигналов от разных радиоцепей пройдет со слегка различающейся поляризацией. Это может быть сделано путем выравнивания или ориентирования антенн так, чтобы путь, который пройдет сигнал, хоть чуть-чуть отличался. Это поможет добавить задержку между различными MIMO сигналами, которая улучшит способность MIMO приемника обработать различные сигналы. Различные типы MIMO антенн обсуждаются в следующем разделе, а технология MIMO исследуется более детально в Главе 10, так как это ключевая компонента в современных W-Fi радиоустройствах.

## MIMO Антенны

С необходимостью и желанием увеличить пропускную способность и емкость беспроводной сети, установка точек доступа с поддержкой MIMO стала нормой. Технология MIMO является стандартом для внутренних сетей, и для внешних сетей, и для сетей точка-точка. Выбор и размещение антенн MIMO являются важными для каждой из этих сред.

### Антенны MIMO для помещений

Обычно не много принимающих решения задумываются об антennaх MIMO точек доступа для помещений. У большинства точек доступа для помещений уровня предприятия есть антенны, встроенные в шасси точки доступа, и эти антенны не выступают из точки доступа. Если антенны не интегрированы в шасси точки доступа, то вероятно точка доступа имеет три или четыре всенаправленные антенны, прямо прикрепленные к ней. В некоторых случаях, антенны являются съемными, позволяющие вам выбрать вместо них всенаправленные антенны с большим усилением или MIMO патч-антенны для помещений.

### Антенны MIMO вне помещений

Также как и для внутренних точек доступа, многолучевое распространение обеспечивает преимущества для успешной и более высокоскоростной связи для уличных MIMO устройств. Это преимущество может оказаться нереализованным, если среда не имеет отражающих поверхностей, которые приводят к многолучевому распространению. Поэтому важно попытаться изменить траекторию излучения антенн, сохранив при этом одинаковую дальность и покрытие для всех антенн. Во внешней среде достижение этой цели требует больше знаний и технологий, чем обычно можно получить, оставив выбор антенн и место ее установки проектировщику или установщику сети. Поэтому, многие производители точек доступа и антенн разработали и всенаправленные, и направленные MIMO антенны.

Чтобы различить сигналы друг от друга от различных радио цепей, направленные MIMO антенны объединяют несколько антенных элементов внутри одной физической антенны. Такая антenna будет иметь два, три или четыре разъема для подключения точки доступа. Если точка доступа, к которой подключена антenna, является точкой доступа с несколькими радиомодулями, то точка доступа будет иметь несколько антенных разъемов для каждого радиомодуля. Важно удостовериться, что кабели от антенн подключены к антенным гнездам одного и того же радиомодуля.

Чтобы обеспечить всенаправленное MIMO покрытие точками доступа с несколькими радио цепями, существует специальный набор антенн. Каждый набор состоит из одной всенаправленной антенны с вертикальной поляризацией и второй всенаправленной антенны с горизонтальной поляризацией. Немного странно использовать эти антенны, потому что в прошлом для старых не-MIMO точек доступа, если две всенаправленные антенны были установлены на точке доступа, то важно было приобретать такие же антенны. Для уличных всенаправленных MIMO антенн, антенны приобретаются как набор, но они обычно имеют разные длину и ширину, из того, что каждая антенна имеет разную поляризацию. Если вы не знакомы с такими новыми антенными парами, вы можете подумать, что вам прислали неправильный товар, из-за того что антенны выглядят не одинаково. Когда вы пытаетесь обеспечить всенаправленное покрытие, существуют специальные антенны с одним шасси, которые могут быть использованы с MIMO точками доступа. Один специальный тип, который называется как *антенна с наклоном вниз [downtilt antenna]*, сделана из нескольких антенных элементов, смонтированных внутри одного антенного корпуса. Антенна обычно устанавливается где-то высоко, устанавливается горизонтально над зоной покрытия, и направляется на пол и землю вниз. Горизонтальная зона покрытия - всенаправленная. Вертикальное покрытие ведет себя как обычная всенаправленная антенна, но с большим вертикальным сигналом/покрытием ниже антенны, по сравнению с сигналом над антенной.

## Соединение и Установка Антennы

В дополнение к физической антенне, являющейся жизненно важным компонентом в беспроводной сети, установка и соединение антенны к беспроводному приемопередатчику является критичным. Если антенна не правильно подключена и установлена, любое преимущество, которое может эта антенна дать сети, может быть мгновенно стерто. Три ключевых компонента связаны с правильной установкой антенны - это коэффициент стоячей волны по напряжению (КСВН или VSWR), потеря сигнала, и фактическое крепление антенны.

### Коэффициент Стоячей Волны по Напряжению

*Коэффициент стоячей волны по напряжению (КСВН) [Voltage standing wave ratio (VSWR)]* это параметр изменения в волновых сопротивлениях к сигналу переменного тока. Стоячие волны по напряжению существуют из-за несовпадающих (несогласованных) или разных волновых сопротивлениях (импедансах) между устройствами в системе радиосвязи. Волновое сопротивление - это значение в омах электрического сопротивления к сигналу переменного тока. Стандартная единица измерения электрического сопротивления ом, названа в честь немецкого физика Георга Ома. Когда передатчик генерирует переменный радиосигнал, сигнал проходит по кабелю до антенны. Часть этой исходящей (или направленной прямо от передатчика к антенне) энергии отражается обратно в передатчик из-за несовпадения волновых сопротивлений.

Несогласованность может произойти на любом участке пути сигнала, но обычно это происходит из-за резкого изменения волнового сопротивления между радиопередатчиком и кабелем и между кабелем и антенной.

Количество отраженной энергии зависит от уровня несогласованности между

передатчиком, кабелем и антенной. Отношение между напряжением отраженной волны и напряжением исходящей волны в одной и той же точке кабеля, называется *коэффициентом отражения по напряжению [voltage reflection coefficient]*, обычно обозначаемым греческой буквой  $\rho$  ( $\rho$ ).

В идеальной системе, где нет несогласованности (волновое сопротивление одинаково везде), вся исходящая энергия дойдет до антенны (кроме потерь на сопротивлении в самом кабеле), и не будет никакой отраженной энергии. Кабель считается *согласованным [matched]*; коэффициент отражения по напряжению точно равен нулю; а *обратные потери [return loss]* в дБ бесконечны. Обратные потери - это, по сути, разница в дБ между мощностью, передаваемой на antennу, и мощностью, отраженной обратно; большее значение лучше чем меньшее значение. Комбинация исходящих и отраженных волн, перемещающихся вперед и назад по кабелю, создает результирующую картину *стоячей волны [standing wave]* по всей длине линии. Форма стоячей волны является периодической (она повторяется) и представляет множество пиков и впадин по напряжению, току и мощности.

KCBH [VSWR] является численной взаимосвязью между максимальным значением напряжения на линии (которое создается передатчиком) и минимальным значением напряжением на линии (которое доходит до антенны). Как показано в уравнении, KCBH (VSWR) является таким образом отношением несогласованности волновых сопротивлений, с оптимальным отношением 1:1 (нет волнового сопротивления), но не достижимым, типовой диапазон значений от 1.1:1 до 1.5:1. KCBH для военных 1.1:1.

$$\text{VSWR} = V_{\max} \div V_{\min}$$

Когда волновые сопротивления передатчика, кабеля, и антенны согласованы (то есть нет стоячих волн), напряжение по всей длине кабеля будет постоянным. Такой согласованный кабель также называется *регулярной линией [flat line]*, потому что нет пиков и впадин напряжения по всей длине кабеля. В этом случае КСВН (VSWR) равен 1:1. По мере роста степени несогласованности, КСВН увеличивается в соответствии с уменьшением мощности, доходящей до антенны. Таблица 5.2 показывает этот эффект.

**ТАБЛИЦА 5.2** Уменьшение сигнала вызванное КСВН (VSWR)

KСВН (VSWR)	Излученная мощность	Потерянная мощность	Обратное затухание (потери)	Потеря мощности в дБ
1:1	100%	0%	Бесконечное	0 дБ
1.5:1	96%	4%	14 дБ	Около 0 дБ
2:1	89%	11%	9.5 дБ	< 1 дБ
6:1	50%	50%	2.9 дБ	3 дБ

Если КСВН(VSWR) большой, это значит, что большое напряжение отражается обратно к передатчику. Это, конечно, означает уменьшение по мощности или амплитуде (затухание) сигнала, который предполагалось передать. Это затухание амплитуды прямого сигнала называется *обратные потери [return loss]*, и могут быть измерены в дБ. Дополнительно, мощность, отраженная обратно, направляется в передатчик. Если передатчик не защищен от избыточной отраженной мощности или больших пиков напряжения, он может перегреться и сломаться. Учтите, что КСВН может привести к уменьшению силы сигнала, непредсказуемости силы сигнала, или даже к поломке передатчика.

Первая вещь, которую можно сделать, чтобы уменьшить КСВН - это проверить, что волновые сопротивления всего сетевого беспроводного оборудования совпадают (согласованы). Большая часть оборудования беспроводных сетей имеет волновое сопротивление 50 ом; однако, проверяйте документацию, чтобы убедиться в этом. При соединении различных компонентов, проверяйте, что все разъемы установлены и завинчены правильно, и что они плотно затянуты.

## Затухание Сигнала

При подключении антенны к передатчику, основная цель, это обеспечить, чтобы как можно больше сигнала, сгенерированного передатчиком, было принято антенной для передачи. Чтобы достичь этого, важно уделить особое внимание кабелям и разъемам, которые соединяют передатчик с антенной. В разделе "Антенные аксессуары" позже в этой главе мы рассмотрим кабели, разъемы(соединители), и много других компонентов, которые используются во время установки антенн. Если используются компоненты низкого качества, или если компоненты неправильно установлены, то вероятнее всего точка доступа будет работать ниже своих оптимальных возможностей.

## Установка Антennы

Как ранее упоминалось, правильная установка антенны является одной из наиболее важных задач для обеспечения оптимального функционирования сети. Следующие пункты являются ключевыми вопросами при установке антенн:

- Расположение(Место установки)
- Монтаж
- Надлежащее использование и окружающая среда
- Ориентация и юстировка
- Безопасность
- Обслуживание

### Расположение(Место установки)

Правильное место установки антенны зависит от типа антенны. Всенаправленные антенны обычно размещают в центре той области, где требуется покрытие. Помните, что всенаправленные антенны с низким усилением дают более широкое вертикальное покрытие, в то время как всенаправленные антенны с высоким усилением дают меньшее вертикальное покрытие. Будьте внимательны, не размещайте всенаправленную антенну с высоким усилением высоко над землей, так как узкое вертикальное покрытие может привести к тому, что антenna даст недостаточный сигнал клиентам, расположенным на земле.

При установке направленных антенн, убедитесь, что вы знаете и горизонтальную и вертикальную ширину луча, так чтобы вы могли правильно нацелить антенну. Также убедитесь, что вы знаете, какое усиление антенны добавляется к передаче. Если сигнал слишком сильный, он пройдет значительно дальше области, которую вам нужно покрыть. Это может быть риском по безопасности,

и вы можете захотеть уменьшить мощность, которую передатчик генерирует, чтобы уменьшить зону покрытия, при условии, что это уменьшение сигнала не влияет на производительность вашей линии связи. В дополнение к тому, что это является риском по безопасности, выход за пределы зоны покрытия считается грубостью.

Если вы устанавливаете внешнюю направленную антенну, в дополнение к вопросам о горизонтальной и вертикальной ширине луча, убедитесь, что у вас на руках корректные расчеты зоны Френеля, и антenna установлена соответственно.

## **Вопросы при монтаже в помещениях**

После принятия решения о том, где разместить антенну, следующий шаг - это принять решение как ее смонтировать. Существует много способов монтажа антенн внутри помещений. У большинства точек доступа есть, как минимум, отверстия для подвешивания точки доступа на пару шурупов на стене. У большинства точек доступа уровня предприятия есть монтажные наборы, которые позволяют вам установить точку доступа на стене или потолке. Многие из этих наборов спроектированы для простого крепления прямо к металлическим направляющим подвесного потолка.

Два общих вопроса - это эстетический вид и безопасность. Многие организации, особенно те, что предоставляют услуги связанные с проживанием, такие как отели и больницы, заботятся об эстетическом виде установки антенн. Специальные короба и потолочные плиты могут помочь скрыть установку точек доступа и антенн. Другие организации, особенно школы, заботятся о безопасности точек доступа и антенн от краж или вандализма. Точка доступа может быть установлена в защищенном корпусе, с коротким кабелем, соединяющим ее с антенной. Если вопрос в безопасности, установка точки доступа высоко на стене или потолке может также минимизировать несанкционированный доступ.

Если точки доступа или антенные установлены ниже потолка, дети или подростки часто пытаются допрыгнуть и ударить антены или бросить что-нибудь в них в попытке сдвинуть их. Это также надо принять во внимание при выборе мест установки антенн.

## **Вопросы при монтаже на улице**

Много антенн, особенно внешних антенн, устанавливаются на мачты или башни. Обычно используют монтажные хомуты или болты в форме U, чтобы прикрепить антены к мачте. Для установки направленных антенн доступны специально разработанные поворотно-откидные монтажные комплекты, облегчающие наведение и фиксацию антены. Если антenna устанавливается на ветреном месте (и какая крыша или башня не ветряная?), убедитесь что вы приняли в расчет ветровую нагрузку и соответствующим образом зафиксировали антенну.

## **Надлежащее использование и окружающая среда**

Убедитесь, что внутренние точки доступа и антены не используются для наружной связи. Внешние точки доступа и антены специально построены чтобы выдержать широкий диапазон температур, которым они могут подвергнуться. Важно убедиться, что окружающая среда, где вы устанавливаете оборудование, находилась в пределах рабочих температур точки доступа и антенн. Экстремально холодная погода северной Канады может быть слишком холодной для некоторого оборудования, в то время как экстремальная жара пустыни в Саудовской Аравии может быть слишком горячей.

Внешние точки доступа и антенны также построены, чтобы выстоять перед другими такими факторами, как дождь, снег и туман. В дополнение к установке соответствующего устройства, убедитесь, что крепеж, который вы используете, предназначен для окружающей среды, в которой вы устанавливаете оборудование.

С расширением беспроводных сетей стало обычным делом устанавливать беспроводные устройства не только в суровых условиях, но и в потенциально огнеопасных или легковоспламеняющихся средах, таких как шахты и нефтяные вышки. Установка точек доступа и антенн в этих условиях требует специальной конструкции устройств или установки устройств в специальные корпуса.

В следующих разделах вы узнаете о четырех классификационных стандартах. Первые два стандарта определяют как устройство будет оставаться в рабочем состоянии в суровых условиях, а следующие два стандарта определяют окружающие среды, в которых устройству разрешается работать. Это просто четыре примера стандартов, которые существуют, и как они применяются к оборудованию и окружающей среде. Вам нужно провести исследование, чтобы определить: существуют ли требования, которые вы должны (или вам следует) придерживаться в вашей стране, регионе, или среде, где устанавливается оборудование.

### **Рейтинг Защиты от Проникновения (IP)**

Рейтинг Защиты от Проникновения [*Ingress Protection Rating*] иногда называется как Рейтинг Международной Защиты [*International Protection Rating*] и обычно называется как *IP Код* [*IP Code*] (не путать с Интернет Протоколом (*Internet Protocol*), который является частью TCP/IP). Система Рейтинга IP опубликована Международной Электротехнической Комиссией (МЭК, или по англ. IEC). IP Код представлен буквами IP, за которыми следуют две цифры или цифра и одна или две буквы, например IP66.

Первая цифра IP кода классифицирует степень защиты, которую обеспечивает устройство от проникновения твердых объектов, вторая цифра классифицирует степень защиты, которую обеспечивает устройство от проникновения воды. Если не обеспечивается никакой защиты ни по одной из этих классификаций, цифра замещается латинской буквой *X*.

Цифра для твердых объектов может принимать значения от 0 до 6, с рейтингом защиты в диапазоне от "нет защиты" (0) до "пыленепроницаемый" (6). Цифра для жидкостей может принимать значения от 0 до 9, включая, например, нет защиты (0), капающая вода (1), брызги воды с любого направления (4), мощная водяная струя (6), погружение более одного метра (8), и водяные струи высокого давления и высокой температуры.

### **Степени защиты корпуса NEMA**

Рейтинг корпусов NEMA [*NEMA Enclosure Rating*] опубликован Национальной Ассоциацией Производителей Электрооборудования США (U.S. National Electrical Manufacturers Association - NEMA). Рейтинг NEMA похож на IP рейтинг, но рейтинг NEMA также определяет и другие характеристики, такие как устойчивость к коррозии, устаревание уплотнителя, назначение и использование устройства.

Типы корпусов NEMA определены в публикации стандартов NEMA 250-2018, "Корпуса Электрооборудования (С максимальным напряжением до 1000 Вольт)". Этот документ определяет степень защиты от таких вещей как: посторонний твердый

предмет, например: грязь, пыль, ворсинки и волокна, а также от попадания воды, масла, и охлаждающей жидкости. Рейтинг корпусов NEMA представлен в виде числа или числа с буквой после нее, например: Тип 2 (Type 2) или Тип 12К (Type 12 K).

Корпуса NEMA, как тот, что показан на Рисунке 5.21, часто нужен, чтобы защитить внешние точки доступа от погодных условий. Многие производители БЛВС также производят внешние точки доступа, которые уже имеют степень защиты NEMA.

#### Р И С У Н О К 5.21 корпус NEMA

Изображение предоставлено компанией Вентев (Ventev) ([www.ventevinfra.com](http://www.ventevinfra.com)).



#### Директивы ATEX

Существуют две директивы ATEX (произносится как "атекс"):

**ATEX 2014/34/EU** Это ревизия ранней директивы ATEX 94/9/ЕС, она вступила в силу 20 Апреля 2016 года. ATEX 2014/34/EU относится к оборудованию и системам защиты, которые предназначены к использованию в потенциально взрывоопасной атмосфере.

**ATEX 137** Также называется как директива ATEX 99/92/ЕС, ATEX 137 относится к рабочему месту, и предназначена для защиты и улучшения безопасности и здоровья рабочих от риска во взрывоопасной атмосфере.

Организации в Европейском Союзе должны следовать этим директивам для защиты сотрудников. Директивы ATEX берут свое название от Французского названия директивы 94/9/EC: "Appareils destinés à être utilisés en Atmosphères Explosibles.", что в переводе значит "Устройства, предназначенные для использования во взрывоопасных средах."

Работодатели должны классифицировать рабочую область, где может существовать взрывоопасная среда, на разные зоны. Области могут быть поделены на газ-пар-туманные среды или на пылевые среды. Эти нормы применяются ко всему оборудованию, и механическому и электрическому, и делятся на шахтное и поверхностное производства. Блоки корпусов ATEX часто нужны в такой среде по очевидным причинам безопасности.

### Опасные места по Национальному Электротехническому Кодексу

Национальный Электротехнический Кодекс [*National Electrical Code (NEC)*] - это стандарт по безопасной установке электрического оборудования и проводки. Сам документ не является юридически обязывающим документом, но он может быть принят и был принят многими местными органами власти и правительствами штатов в Соединенных Штатах, делая его законом локально. Существенная часть NEC обсуждает опасные места. NEC классифицирует места по типу, условиям и природе. Тип опасного места определяется следующим образом:

- **Класс I:** Газ или пар
- **Класс II:** Пыль
- **Класс III:** Волокна и пух

Тип далее подразделяется по условиям опасных мест:

- **Категория 1:** Обычные условия (например, обычный день в погрузочном доке)
- **Категория 2:** Необычные условия, которые происходят от 0.1 до 10% времени (тот же самый погрузочный док, но контейнер с вытекающим содержимым)

Финальная классификация определяет группу опасных веществ, на основе природы вещества. Это значение представляется заглавной буквой английского алфавита в диапазоне от A до G.

### Ориентация и юстировка

Перед установкой антенны, убедитесь, что вы прочитали рекомендации производителя по ее монтажу. Это предложение особенно важно при установке направленных антенн. Так как направленные антенны могут иметь разную горизонтальную и вертикальную ширину луча, а из-за того, что направленные антенны могут быть установлены с разной поляризацией, соответствующая ориентация может дать большую разницу между возможностью установить связь и нет:

1. Убедитесь, что поляризация антенны одинакова на обоих концах направленного канала связи.
2. Определитесь со способом монтажа и убедитесь, что он соответствуют месту монтажа.
3. Отьюстируйте антенны. Помните, что вам нужно отьюстрировать и по горизонтальному направлению антенны и по ее вертикальному углу наклона.
4. Защитите от погодных условий кабели и соединители, а также прикрепите их, чтобы они не болтались.

5. Задокументируйте и сфотографируйте каждую установку точки доступа и антенн. Это поможет вам при устраниении проблем в будущем и позволит вам легче определить есть ли сдвиг при установке или выравнивании антенны.

Как уже ранее упоминалось, с переходом на радиомодули MIMO, специальные с двумя радио цепями уличные всенаправленные MIMO антенны спроектированы для того, чтобы устанавливаться парой, где одна антenna создает сигнал с вертикальной поляризацией, а другая создает сигнал с горизонтальной поляризацией.

## Безопасность

Мы не можем не подчеркнуть важность быть осторожным при установке антенн. Большую часть времени установка антенн требует взбираться по лестницам, башням или крышам. Гравитация и ветер могут усложнить установку как для того, кто забирается наверх, так и для людей внизу, помогающих ему.

Распланируйте установку заранее, убедитесь, что у вас есть все необходимые инструменты и оборудование для установки антены. Незапланированные остановки установки и перемещения забытого оборудования вверх и вниз по лестнице увеличивают риск получения травм.

Будьте осторожны когда работаете с вашей антенной вблизи других антенн. Узконаправленные антенны фокусируют радиоволновую энергию высокой концентрации. Это большое количество энергии может быть опасно для вашего здоровья. Не включайте вашу antennу, пока вы с ней работаете, и не стойте перед другими антеннами, которые находятся рядом с местом установки вашей антены. Вероятнее всего вы не знаете ни выходную частоту или мощность этих других антенных систем, ни потенциального риска для здоровья, которому вы можете подвергнуться.

При установке антенн (или любого устройства) на потолках, стропилах, или мачтах, убедитесь, что они соответствующим образом закреплены. Даже однофунтовая (1 фунт = 453,6 грамма) антена может быть смертельной, если она упадет со стропил складского помещения.

Если вы будете устанавливать антены как часть вашей работы, мы рекомендуем, чтобы вы прошли курс по охране труда и технике безопасности при работе с радиоустановками. В Соединенных Штатах, эти курсы научат вас нормам FCC и Управлением по Охране Труда Министерства Труда США (OSHA), и как быть в безопасности и соответствовать стандартам. Аналогичные курсы можно найти во многих других странах по всему миру. Мы советуем поискать курсы, которые соответствуют вашей стране или региону.

Если вам нужно установить antennу на любой возвышенной структуре, например: столбе, башне или даже крыше, рассмотрите возможность найма профессионального установщика. Профессиональные альпинисты и установщики – подготовлены и, в некоторых местах сертифицированы выполнять такие типы установок. Кроме подготовки, у них есть необходимое оборудование по обеспечению безопасности и соответствующий полис страхования для работы.

Если вы планируете установку беспроводного оборудования в качестве профессии, вам следует разработать инструкцию по охране труда, одобренную вашим местным представителем по охране труда. В России вам не нужно согласовывать инструкцию по охране труда с трудовой инспекцией, однако она должна быть актуальной и соответствовать действующему законодательству. Вам также следует пройти

аккредитованные курсы по охране труда при работе на высоте в дополнение к курсам по охране труда при работе с радиоустановками. Также настойчиво рекомендуем пройти курсы по оказанию первой медицинской помощи и сердечно-легочной реанимации (т.н. «искусственное дыхание»). В России охрана труда при установке и обслуживании радиоустановок регламентируется Приказом Минтруда РФ от 07.12.2020 N 867Н "Об утверждении Правил по охране труда при выполнении работ на объектах связи". Таким образом вам нужно будет пройти курсы по охране труда, по электробезопасности, скорее всего иметь III или IV группу электробезопасности, пройти курсы по работе на высоте и получить соответствующие удостоверения.

## Обслуживание

Существует два типа обслуживания: превентивное и диагностическое. При установке антенн важно предотвратить появление проблем в будущем. Это кажется просто советом, но так как до антенн часто трудно добраться после того, как они установлены, это особо предусмотрительный совет. Две ключевые проблемы могут быть минимизированы при соответствующих превентивных мерах – это повреждения от ветра и повреждения от воды. При установке антennы убедитесь, что все гайки, болты, винты и т. д. установлены и затянуты должным образом. Также убедитесь, что все кабели надежно закреплены, чтобы их не мотало ветром.

Чтобы помочь предотвратить повреждения от воды, можно использовать холодную усадку или ленту-герметик для коаксиальных соединений чтобы минимизировать риск попадания воды в кабель или разъемы. Еще один распространенный метод - это комбинация изоленты и мастики, устанавливаемых послойно, чтобы обеспечить полностью водонепроницаемую установку. Если используете мастику, обязательно сначала плотно обмотайте соединение изолентой, прежде чем применять мастику. Если соединение когда-нибудь нужно будет разъединить и соединить снова, то фактически невозможно удалить мастику, если она была нанесена прямо на разъем.



Не следует использовать термоусадку, так как можно повредить кабель высокой температурой, которая нужна для усадки трубы. Также не стоит использовать силиконовый герметик, так как под ним могут образоваться воздушные пузырьки и туда может попасть влага.

Еще один способ прокладывания кабеля - это капельная петля. Чтобы сделать капельную петлю, когда кабель спускается вниз к разъему, проложите кабель ниже разъема и затем разверните кабель вверх к разъему, создавая таким образом небольшую петлю в виде подковы или буквы "U" кабелем, который ниже разъема. Капельная петля также используется при вводе кабеля в здание или сооружение. Капельная петля предотвращает попадание воды, стекающей вниз по кабелю, в разъем или отверстие входа кабеля в здание. Вода, которая течет вниз по кабелю, продолжит течь до нижней точки петли и затем будет капать вниз.

Антенны обычно установлены и забыты, до тех пор пока они не сломаются. Рекомендуется периодически проводить визуальную инспекцию антенн и, если необходимо, сверять ее статус с документацией по установке. Если антenna не доступна так просто, то бинокль или фотоаппарат с очень высоким оптическим приближением упростят задачу.

# Антенные Аксессуары

В Главе 4 мы представили основные компоненты радиосвязи. Существуют дополнительные компоненты, которые не так значимы и не всегда устанавливаются как часть канала связи. Важные характеристики для всех антенных аксессуаров включают: частотную характеристику, волновое сопротивление, КСВН, максимальную входную мощность, и вносимые потери. Мы обсудим некоторые из этих компонентов и аксессуаров в следующих разделах.

## Кабели

Неправильная установка или выбор кабелей может губительно повлиять на радиосвязь больше чем любой другой компонент или внешнее воздействие. Важно помнить этот факт при установке антенных кабелей. В следующем списке рассматриваются некоторые вопросы, связанные с выбором и установкой кабелей:

- Убедитесь в выборе корректного кабеля.  
Волновое сопротивление кабеля должно совпадать с волновым сопротивлением антенны и приемопередатчика. Если есть несовпадение волновых сопротивлений, то возвратные потери от КСВН будут действовать на канал связи.
- Убедитесь, что кабель, который вы выбрали, поддерживает частоты, которые вы будете использовать.  
Как правило, производители кабелей указывают срез частот, которые представляют собой самые низкие и самые высокие частоты, поддерживаемые кабелем. Это называется частотная характеристика. Например, кабель LMR - популярная марка коаксиального кабеля, используемого в радиосвязи. LMR-1200 не работает с 5ГГц передачей. LMR-900 это самый высокий номер, который вы можете использовать. Однако, для работы в 2,4ГГц вы можете использовать LMR-1200.

- Кабель вносит потери сигнала в канале связи.

Производители кабелей предоставляют таблицы и калькуляторы, чтобы помочь вам определить величину потерь. Рисунок 5.22 представляет собой таблицу затуханий для кабеля LMR, производимого Таймз Майкровэйв Системз (Times Microwave Systems). Левая сторона таблицы перечисляет различные типы кабеля LMR. Чем ниже по списку, тем лучше кабель. Более качественный кабель обычно толще, жестче, с ним труднее работать и, конечно же, он дороже. Таблица показывает сколько децибел потерь в кабеле добавится к каналу связи на каждые 100 футов кабеля. Заголовки колонок перечисляют частоты, которые могут быть использованы с кабелем. Например: 100 футов кабеля LMR-400, используемого на сети 2.5ГГц (2500МГц), уменьшит сигнал на 6,8дБ.

- Затухание увеличивается с частотой. Если вы переделываете БЛВС 2,4ГГц в БЛВС 5ГГц, потери создаваемые кабелем будут больше.
- Или покупайте уже нарезанный и с установленными разъемами кабель, или найдите профессионального кабельщика, чтобы установить соединения (ну пока вы сами не являетесь профессиональным кабельщиком).

Неправильно установленные разъемы внесут больше потерь в канал связи., что может обнулить излишне потраченные деньги на покупку более

качественного кабеля. Также они могут добавить обратные потери в кабеле из-за отражений.

## Разъемы

Большинство тех же самых принципов, касающихся кабеля, применимы и к разъемам, а также к другим аксессуарам. Радио разъемы (ВЧ-разъемы) должны быть с корректным волновым сопротивлением, чтобы соответствовать другому радио оборудованию. Они также поддерживают определенный диапазон частот. Разъемы вносят потери сигнала в радиоканал, и разъемы низкого качества более вероятно вызовут проблемы со связью или КСВН. ВЧ-разъемы в среднем добавляют по 1/2 дБ потерь.

### РИСУНОК 5.22 Затухание коаксиального кабеля

Times Microwave Systems (Затухание дБ/100 футов)											
Кабель LMR\Частота	30	50	150	220	450	900	1,500	1,800	2,000	2,500	5,800
100A	3.9	5.1	8.9	10.9	15.8	22.8	30.1	33.2	35.2	39.8	64.1
195	2	2.5	4.4	5.4	7.8	11.1	14.5	16	16.9	19	29.9
195UF	2.3	3	5.3	6.4	9.3	13.2	17.3	19	20.1	22.6	35.6
200	1.8	2.3	4	4.8	7	9.9	12.9	14.2	15	16.9	26.4
200UF	2.1	2.7	4.8	5.8	8.3	11.9	15.5	17.1	18	20.2	31.6
240	1.3	1.7	3	3.7	5.3	7.6	9.9	10.9	11.5	12.9	20.4
240UF	1.6	2.1	3.6	4.4	6.3	9.1	11.8	13	13.8	15.5	24.4
300	1.1	1.4	2.4	2.9	4.2	6.1	7.9	8.7	9.2	10.4	16.5
300UF	1.3	1.6	2.9	3.5	5.1	7.3	9.5	10.5	11.1	12.5	19.8
400	0.7	0.9	1.5	1.9	2.7	3.9	5.1	5.7	6	6.8	10.8
400UF	0.8	1.1	1.8	2.2	3.3	4.7	6.2	6.8	7.2	8.1	13
500	0.5	0.7	1.2	1.5	2.2	3.1	4.1	4.6	4.8	5.5	8.9
500UF	0.6	0.8	1.5	1.8	2.6	3.8	5	5.5	5.8	6.6	10.6
600	0.4	0.5	1	1.2	1.7	2.5	3.3	3.7	3.9	4.4	7.3
600UF	0.5	0.7	1.2	1.4	2.1	3	4	4.4	4.7	5.3	8.7
900	0.3	0.4	0.7	0.8	1.2	1.7	2.2	2.5	2.6	3	4.9
1200	0.2	0.3	0.5	0.6	0.9	1.3	1.7	1.9	2	2.3	Не поддерживается
1700	0.1	0.2	0.3	0.4	0.6	0.9	1.3	1.4	1.5	1.7	Не поддерживается

UF = Ультрафлекс (более гибкий кабель)

## Делители

Делители (*Splitters*) также называют как делители сигналов, антенные разветвители, сплиттеры, сумматоры, ВЧ- и СВЧ- делители, делители мощности. Делитель - это разъем или кабель, который делит радиосигнал на два или более отдельных сигналов. Только в необычной особой или уникальной ситуации вам возможно понадобится использовать ВЧ-делитель. Когда вы устанавливаете делитель, сигнал не только ухудшается из-за его разделения (называется *сквозные потери [through loss]*), но также каждый разъем добавляет к сигналу свои собственные вносимые потери. Существует так много переменных и потенциальных проблем с этой конфигурацией, что мы рекомендуем выполнять такой тип установки только человеку, хорошо разбирающемуся в радио, и только как временные решения.

Более практическое, но опять же редкое использование делителя – это мониторинг передаваемой мощности. Делитель может быть подключен к приемопередатчику, а затем к

антенне и измерителю мощности. Такой подход позволит вам активно мониторить мощность, отправляемую антенне.

## Усилители

*ВЧ усилитель [RF amplifier]* получает сигнал, создаваемый приемопередатчиком, усиливает его, и отправляет к антенне. В отличие от антенны, обеспечивающей увеличение в усилении путем фокусировки сигнала, усилитель обеспечивает общее увеличение по мощности путем добавления электрической энергии к сигналу, это называется *активным усилением [active gain]*.

Усилители можно приобрести как однонаправленные, так и двунаправленные устройства. Однонаправленные усилители выполняют усиление только в одном направлении, или когда передают, или когда принимают. Двунаправленные усилители производят усиление в обоих направлениях.

Увеличение по мощности усилителем создается одним из следующих двух методов:

**Фиксированное Усиление [Fixed-Gain]** В методе фиксированного усиления выходной сигнал приемопередатчика увеличивается на определенную величину усилителя.

**Фиксированная Выходная Мощность [Fixed-Output]** Усилитель с фиксированной выходной мощностью не добавляет ничего к выходному сигналу трансивера. Он просто генерирует точно такой же сигнал на выходе усилителя, независимо от мощности, созданной приемопередатчиком.



Усилители с регулируемым усилением также существуют, но их использование на практике не рекомендуется. Некомпетентная настройка усилителя с регулируемым усилением может привести как к нарушению разрешенной нормами мощности, так и недостаточной амплитуде передачи.

Поскольку большинство регулирующих организаций ограничивают максимальную нормативную мощность в 1 Ватт или меньше в точке расчетного излучателя (IR), то основная цель использования усилителя - компенсировать затухание в кабеле, а не усиление сигнала. Следовательно, если вы устанавливаете усилитель, ставьте его как можно ближе к антенне. Так как антенный кабель вносит потери сигнала, чем короче антенный кабель, тем меньше он внесет потерь и тем больший сигнал достанется антенне.

Также, важно отметить, что усилитель увеличивает шум также как и силу самого сигнала. Не является чем то необычным для усилителя увеличение уровня шума на 10dB или больше.



Обычно усилители должны быть сертифицированы с используемой системой, в соответствии с регулирующими органами, таким как FCC. Если усилитель добавлен в беспроводную сеть и не был сертифицирован, то он нелегален. Намного лучше инженерно доработать систему, чем использовать усилитель.

## Аттенюаторы

В некоторых ситуациях, может быть необходимо уменьшить величину сигнала, которая излучается антенной. В некоторых случаях, даже установка самой маленькой мощности на приемопередатчике может генерировать сигнал больше, чем нужно. В этой ситуации вы можете добавить *аттенюатор [attenuator]* с фиксированным затуханием или с регулируемым затуханием.

. Обычно аттенюаторы - это небольшие устройства размером примерно с большую "круглую" батарейку (Батарейка типа С) или меньше, с кабельными разъемами с обеих сторон. Аттенюатор поглощает энергию, уменьшая сигнал при прохождении через него. Аттенюаторы с фиксированным затуханием обеспечивают затухание определенной величины дБ. У аттенюаторов с регулируемым значением затухания есть циферблат или переключатель конфигурации, который позволяет вам настроить количество поглощаемой энергии.

Аттенюаторы с регулируемым затуханием могут быть использованы при уличном радиоисследовании, чтобы эмулировать потери, вызванные кабелем различного качества и различными длинами кабелей. Еще одно интересное применение аттенюатора с регулируемым затуханием это проверить реальный запас на замирания на канале точка-точка. Постепенно увеличиваете затухание до тех пор пока канал не пропадет, далее вы можете использовать это значение, чтобы определить реальный запас на замирание этого канала связи.

## Грозоразрядники (молниезащита)

Назначение грозоразрядника (грозозащиты, или молниезащиты) [*lightning arrestor*] - это перенаправить (зашунтировать) кратковременные токи, вызванные ближайшими разрядами молнии или окружающего статического электричества, от ваших электронных устройств в землю. Грозоразрядники используются для защиты электронного оборудования от резкого скачка мощности, который может быть вызван близким ударом молнии или возникшим статическим электричеством. Вы могли обратить внимание на использование фразы "близкого удара молнии". Эта формулировка используется, потому что грозозащита не способна защитить от прямого удара молнии. Грозоразрядники обычно могут защитить от скачка вплоть до 5000 ампер до 50 вольт. IEEE определяет, что грозоразрядники должны быть способны перенаправить кратковременные токи меньше чем за 8 микросекунд. Большинство грозоразрядников способны сделать это меньше чем за 2 микросекунды.

Грозозащита устанавливается между приемопередатчиком и антенной. Любое устройство, установленное между грозозащитой и антенной, не будет защищено грозозащитой. Следовательно, грозозащита обычно ставится как можно ближе к антенне, а все остальные устройства связи (усилители, аттенюаторы, и т.д.) ставятся между грозозащитой и приемопередатчиком. После того как грозозащита сделает свою работу по защите оборудования от электрического скачка, его нужно будет заменить, ну или у него может быть заменяемая газоразрядная трубка (как предохранитель). Большинство инсталляций (установок) размещают грозозащиту на вводе в здание. Комплекты кабельного заземления можно ставить возле антенны и далее каждые 100 футов (30,48 метров).

Оптоволоконный кабель также можно использовать для того, чтобы обеспечить дополнительную защиту от молнии. Небольшой кусок оптоволоконного кабеля можно вставить в Ethernet кабель, который соединяет беспроводной мост с остальной сетью. АдAPTERЫ Ethernet - оптоволокно, называемые медиаконверторы (трансиверы), преобразовывают электрический Ethernet сигнал в световой оптоволоконный сигнал, а

затем обратно в Ethernet. Так как оптоволоконный кабель сделан из стекла и использует свет, а не электричество для передачи данных, то он не проводит электричество. Важно только убедиться, что блок питания адаптера тоже защищен.

Оптоволоконный кабель действует как некоторый вид защитной сети, если грозозащита выйдет из строя из-за очень большого кратковременного тока или даже прямого удара молнии. Имейте в виду, что в случае прямого удара молнии в антенну, вам нужно планировать замену всех компонентов: от оптоволоконного кабеля до антенны. Кроме того, прямой удар молнии может также обогнуть оптоволокно и вызвать повреждения оборудования на другой стороне оптоволоконного канала. Заземление ВЧ кабелей также может помочь предотвратить это происшествие.



## Пример из Реальной Жизни

### Не только молния не предсказуема, но и результат тоже!

Предприятие в пятиэтажном 200-летнем кирпичном доме из коричневого камня в районе Норт-Энд в Бостоне получило удар молнии или удар молнии был где-то рядом. Это здание даже не было самым высоким зданием в округе, и оно было внизу небольшого холма и окружено другими такими же зданиями. Электрический ток прошел вниз по водосточной трубе и мимо пучка Ethernet кабелей. Кратковременный ток в Ethernet кабелях повредил цепи приемопередатчика Ethernet адаптера на персональных компьютерах и отдельных портах Ethernet хаба. Около половины Ethernet устройств в компании вышли из строя, а около половины портов на хабе больше не работали. Тем не менее, все программное обеспечение определяло адаптеры, и все индикаторы питания и портов работали безупречно. Проблема оказалась связана с кабелем.

Вы часто не будете знать, что проблема связана с молнией, а симптомы могут вводить в заблуждение. Проверка грозозащиты сможет помочь вам с диагнозом.

## Заземляющие стержни и провода

Когда молния попадает в объект, она ищет путь наименьшего сопротивления, или более специфично, путь наименьшего полного сопротивления (импеданса). Это как раз где начинает играть оборудование грозозащиты и заземления. Система заземления состоит из заземляющего стержня и проводов, обеспечивающих путь с низким полным сопротивлением до земли. Этот путь с низким полным сопротивлением (низкоимпедансный путь) устанавливается, чтобы помочь молнии пройти именно через него, а не через ваше дорогое электронное оборудование.

Заземляющий стержень и провода также используются, чтобы создать, что называется - *общую землю* [*common ground*]. Один из способов создания общей земли - это погрузить медный стержень в землю и соединить ваше электрическое и электронное оборудование с этим стержнем с помощью проводов или полос (заземляющих проводов). Заземляющий стержень должен быть полностью погружен в землю, оставляя достаточную часть стержня доступной для прикрепления заземляющих проводов к нему. Создавая общую землю, вы создаете путь наименьшего полного сопротивления для всего вашего оборудования, на случай, если молния вызовет скачок электричества.

## Соответствие нормам

Из Главы 4 вы узнали о радиокомпонентах в концепциях расчетного излучателя (IR) и эквивалентной изотропно излучаемой мощности (ЭИИМ или EIRP). В этой главе, вы узнали об антennaх и многих аспектах работы антенн и установки.

И хотя существует много вариантов антенн, кабелей и компонентов, когда вы конфигурируете беспроводную сеть, реальность такова, что вы часто ограничены в выборе антенн из-за регуляторных требований. Хоть каждый регулирующий орган работает независимо, существуют схожести между тем, как эти организации работают и сертифицируют оборудование. Этот раздел кратко объяснит данный процесс в Соединенных Штатах, который регулируется FCC.

Для того чтобы производитель точки доступа продал свой продукт в стране или регионе, он должен доказать что его продукт работает в пределах правил соответствующей регуляторной области, таких как FCC. FCC создает документы, которые определяют правила, которым должен следовать производитель, также называемый как *ответственная сторона [responsible party]* или *основной держатель [grant holder]*. Производитель отправляет свое оборудование на испытания регулирующей организацией или авторизованной испытательной организацией, которая проводит испытания оборудования на соответствие. Если оборудование прошло испытания, устройству выдается идентификационный номер и Сертификат Соответствия.

Большинство людей не знакомы с этим процессом и не осознают, что когда компания отправляет свой продукт на испытания, она отправляет всю систему, которую производитель рекламирует и продает как продукт, который включает расчетный излучатель (радиомодуль точки доступа), все кабели и разъемы, и антенну или антенны, которые он хочет, чтобы работали с точкой доступа. У большинства компаний точки доступа сертифицируются с группой антенн, которые дают различное усиление и ширину луча.

Расчетный излучатель может работать только с антенной, с которой он авторизован (сертифицирован). FCC разрешает заменить antennу на другую, при соблюдении двух ключевых условий:

- Усиление новой антенны должно быть таким же или меньше, чем антенны с которой сертифицировалась система.
- Новая антenna должна быть того же самого типа, что означает, что антenna должна иметь те же самые внутриволосные и внеполосные характеристики.

Усиление антенны легко идентифицируется и обеспечивается многими антennами, таким образом первое условие достаточно просто выполнить. Однако, выполнить второе условие — например, определение того же типа антenna как и другая - требует проверки и внутриволосных и внеполосных характеристик антennы. Как новая антenna будет работать как часть комбинированной системы в отношении к внеполосным требованиям трудно предсказать только по данным из информационного листка [data sheet]. Внеполосные требования обычно включают ограничения прерывистых излучений в очень широкой полосе частот (от 9кГц до 300 ГГц), излучения на краю полосы (требования к типу маски), ограничения на генерируемые гармоники, очень низкие пределы по шуму в определенных запрещенных полосах. Проверка новой антennы по всем этим "внеполосным" требованиям может потребовать настолько обширные испытания как и при оригинальном сертификационном испытании . Следовательно, если вы хотите заменить вашу антенну на антенну стороннего производителя, вам может понадобиться провести работу по тому, чтобы убедиться что использование этих антenn с вашей точкой доступа приемлемо с точки зрения локального регулирования.

## Итого

Эта глава сфокусирована на радиосигнале и теории антенн. Антенна является ключевым компонентом успешной радиосвязи. Следующие четыре типа антенн используются в сетях 802.11:

- Всенаправленные (дипольные, коллинеарные)
- Всенаправленные с уклоном вниз
- Полунаправленные (патч, панель, Яги)
- Узконаправленные (параболическая тарелка, сетчатая)
- Сектор

Разные типы антенн производят различные формы сигналов, которые можно посмотреть на азимутальной диаграмме и диаграмме по углу места.

Эта глава также рассматривает следующие ключевые моменты, требующие внимания при установке связи точка-точка:

- Видимая линия прямой видимости
- Радиоволновая линия прямой видимости
- Зона Френеля
- Выпуклость Земли
- Поляризация Антенны

Последний раздел этой главы рассматривает КСВН и вопросы монтажа антennы, вместе с антennыми аксессуарами и их ролью.

## Темы Экзамена

**Знать различные категории и типы антенн, как они излучают сигналы, и в какой среде они используются.**

Убедитесь, что вы знаете три главные категории антenn и различные типы антenn. Знать схожести и различия между ними, и понимать когда и почему нужно использовать ту или другую антенну. Убедитесь, что вы понимаете азимутальную диаграмму и диаграмму по углу места, ширину луча, поляризацию антennы, и антеннное разнесение.

**Полное понимание Зоны Френеля.** Убедитесь, что вы понимаете все проблемы и нюансы, связанные с установкой канала связи точка-точка. Вам не требуется запоминать формулы зоны Френеля или выпуклости Земли, однако, вам нужно знать принципы, касательно этих тем, и когда и почему вам нужно использовать формулы.

**Понимать проблемы, связанные с подключением и установкой антenn и антennых аксессуаров.** Каждый кабель, разъем, и устройство между приемопередатчиком и антенной влияют на сигнал, который излучается антенной. Понимать, какие устройства обеспечивают усиление, а какие устройства дают затухание. Понимать что такое КСВН, и какие его значения хорошие, а какие плохие. Знать различные антенные аксессуары, что они делают, и почему и когда вам стоит из использовать.

# Контрольные вопросы

1. Что из следующего относится к полярной диаграмме, как если бы вы смотрели на антенну сверху? (Выберите все, что применимо.)
  - A. Горизонтальный вид
  - B. Вертикальный вид
  - C. H-плоскость [H-plane]
  - D. E-плоскость [E-plane]
  - E. Диаграмма по углу места [Elevation chart]
  - F. Азимутальная диаграмма [Azimuth chart]
2. Азимутальная диаграмма представляет вид диаграммы направленности антенны с какого направления?
  - A. Сверху
  - B. Сбоку
  - C. Спереди
  - D. Сверху и сбоку
3. Что является определением горизонтальной ширины луча антенны?
  - A. Мера угла основного лепестка, как показано на азимутальной диаграмме
  - B. Расстояние между двумя точками на горизонтальной оси, где сигнал уменьшается на треть. Это расстояние измеряется в градусах.
  - C. Расстояние между двумя точками -3дБ на горизонтальной оси, измеряемое в градусах
  - D. Расстояние между пиковой мощностью и точкой, где сигнал уменьшается вдвое. Расстояние измеряется в градусах.
4. Какие антенны являются узконаправленными? (Выберите все, что применимо.)
  - A. Патч-антенна
  - B. Панельная антенна
  - C. Параболическая тарелка
  - D. Решетчатая антенна (Grid)
  - E. Секторная антенна
5. Полунаправленные антенны часто используются для каких из следующих целей? (Выберите все, что применимо.)
  - A. Чтобы обеспечить наружную связь точка-точка на короткие расстояния
  - B. Чтобы обеспечить наружную связь точка-точка на длинные расстояния
  - C. Чтобы обеспечить однонаправленное покрытие от точки доступа до клиентов внутри помещений
  - D. Чтобы обеспечить сфокусированное или секторное покрытие в средах с высокой плотностью.

6. Зона Френеля не должна блокироваться на какой процент, чтобы поддерживать надежным канал связи?
- A. 20 процентов
  - B. 40 процентов
  - C. 50 процентов
  - D. 60 процентов
7. Размер зоны Френеля управляется какими факторами? (Выберите все, что применимо.)
- A. Ширина луча антенны
  - B. Линия прямой видимости
  - C. Расстояние
  - D. Частота
8. Когда устанавливается канал связи точка-точка на большое расстояние, выпуклость (изгиб) земли нужно принимать во внимание с расстояния более чем сколько?
- A. 5 миль [ $\sim 8$  км]
  - B. 7 миль [ $\sim 11.27$  км]
  - C. 10 миль [ $\sim 16.09$  км]
  - D. 30 миль [ $\sim 48.28$  км]
9. Сетевой администратор заменил коаксиальный кабель, использовавшийся для подключения внешнего моста, после повреждения кабеля водой. После замены кабеля сетевой администратор заметил, что ЭИИМ (EIRP) значительно увеличился, и возможно нарушает максимальную максимально разрешенную законом мощность ЭИИМ (EIRP). Что является возможной причиной увеличения амплитуды? (Выберите все, что применимо.)
- A. Администратор установил более короткий кабель
  - B. Администратор установил кабель более низкого качества.
  - C. Администратор установил кабель более высокого качества
  - D. Администратор установил более длинный кабель.
  - E. Администратор использовал кабель другого цвета.
10. Что из следующего верно для передачи МИМО?
- A. Приемопередатчик может только принимать от одной антенны одновременно.
  - B. Приемопередатчики могут передавать через несколько антенн одновременно.
  - C. Приемопередатчик записывает сигнал с нескольких антенн и выбирает лучший принятый сигнал с одной антенны.
  - D. Приемопередатчик может передавать только с одной антенны одновременно.
11. Чтобы организовать четырехмилльный радиомост точка-точка в диапазоне U-NII-3 5 ГГц, какие факторы должны быть приняты во внимание? (Выберите все, что применимо.)
- A. Зазор(Клиренс) Зоны Френеля
  - B. Расчет Выпуклости Земли

- C. Регулятивные нормы мощности вне помещений
  - D. Корректный выбор полунаправленных антенн.
  - E. Корректный выбор узконаправленных антенн.
12. Отношение между максимальным пиком напряжения и минимальным напряжением на линии называется как?
- A. Поток радиосигнала
  - B. Возвратные потери
  - C. КСВН
  - D. Исходящие волны сигнала
13. Что является некоторым возможным негативным эффектом несогласованности волновых сопротивлений? (Выберите все, что применимо.)
- A. Отражение напряжения
  - B. Блокировка зоны Френеля
  - C. Непредсказуемая сила сигнала
  - D. Уменьшенная амплитуда сигнала
  - E. Поломка усилителя/передатчика
14. При определении высоты установки антенны точка-точка на далекое расстояние, что из следующего следует принять во внимание? (Выберите все, что применимо.)
- A. Частоту
  - B. Расстояние
  - C. Прямую видимость
  - D. Выпуклость Земли
  - E. Ширину луча антенны
  - F. Радиоволновую прямую видимость
15. Что из нижеследующее является верным относительно кабелей? (Выберите все, что применимо.)
- A. Они вызывают волновое сопротивление на сигнале.
  - B. Они работают независимо от частоты.
  - C. Затухание уменьшается с увеличением частоты.
  - D. Они добавляют потери к сигналу.
16. С какими из следующих характеристик можно купить усилители? (Выберите все, что применимо.)
- A. Двунаправленное усиление
  - B. Однонаправленное усиление
  - C. Фиксированное усиление
  - D. Фиксированный выходная мощность

- 17.** Сигнал между приемопередатчиком и антенной будет уменьшен каким из следующих способов? (Выберите все, что применимо.)
- A.** Добавлением аттенюатора
  - B.** Увеличением длины кабеля
  - C.** Уменьшением длины кабеля
  - D.** Использованием кабеля более дешевого качества
- 18.** Грозозащита будет защищать от чего из нижеперечисленного?
- A.** Прямых ударов молнии
  - B.** Скачков мощности
  - C.** Кратковременных токов
  - D.** Неправильного общего заземления
- 19.** Радиус первой зоны Френеля это \_\_\_\_\_. (Выберите все, что применимо.)
- A.** Внешняя граница области, где сигнал находится не в фазе с точечным источником
  - B.** Внешняя граница области, где сигнал находится в одной фазе с точечным источником
  - C.** Зависит от усиления направленной антенны
  - D.** Меньше чем вторая зона Френеля
- 20.** Во время выравнивания (юстировки) антенны, вы заметили, что сигнал падает когда вы отворачиваетесь антенну от другой антенны, а за тем он немного увеличивается. Это увеличение сигнала наиболее вероятно вызвано чем?
- A.** Отражением сигнала
  - B.** Частотной гармоникой
  - C.** Боковой полосой
  - D.** Боковым лепестком

# Г л а в а

# 6



# Беспроводные Сети и Технологии Расширения Спектра

---

**В ЭТОЙ ГЛАВЕ ВЫ УЗНАЕТЕ О  
СЛЕДУЮЩЕМ:**

- ✓ Пропускная способность против Полосы пропускания
- ✓ Узкополосный сигнал и расширение спектра
  - Интерференция многолучевого распространения
- ✓ Расширение спектра скачкообразной перестройкой частоты
  - Перестроечная последовательность
  - Время передачи
  - Время перестройки
  - Модуляция
- ✓ Расширение спектра прямой последовательностью
  - Кодирование данных DSSS
  - Модуляция
  - Спектральная маска передачи
- ✓ Мультиплексирование с ортогональным частотным разделением
  - Сверточное кодирование
  - Модуляция
  - Спектральная маска передачи
  - Множественный доступ с ортогональным частотным разделением
- ✓ Промышленные, научные и медицинские полосы частот (ISM)
  - Полоса ISM 900 МГц
  - Полоса ISM 2,4 ГГц
  - Полоса ISM 5,8 ГГц



- ✓ Нелицензируемые 5ГГц Полосы Национальной Информационной Инфраструктуры
  - U-NII-1
  - U-NII-2A
  - U-NII-2C
  - U-NII-3
  - U-NII-4
- ✓ 60 ГГц для Wi-Fi
- ✓ Ниже 1 ГГц
- ✓ Каналы 2.4 ГГц
- ✓ Каналы 5 ГГц
  - Долгосрочная эволюция [LTE] в 5ГГц
- ✓ Каналы 6 ГГц
  - Существующее использование 6ГГц
  - Автоматизированная координация частот
    - 6 ГГц в Мире
    - Рассуждения о 6ГГц Wi-Fi



В этой главе вы узнаете о различных технологиях расширения спектра при передаче и частотные диапазоны, которые поддерживаются стандартом 802.11 и поправками. Вы узнаете, как эти частоты поделены на различные каналы, и некоторые правильные и неправильные способы использования каналов.

Дополнительно, вы узнаете о различных типах технологии расширения спектра. Вы также узнаете о мультиплексировании с ортогональным-частотным разделением (OFDM) и сходствами и различиями между OFDM и расширением спектра.

Эта глава содержит много ссылок на спецификации и правила FCC. Экзамен CWNA не проверяет вас ни по какой специфичной для региона регуляторной информации. Любая ссылка на FCC предоставляется только, чтобы помочь вам понять технологию лучше. Важно понимать, что часто существуют сходства между регулирующими органами разных регионов. Соответственно, понимание правил регулятора одной страны может помочь вам понимать правила вашего регулятора вашего региона.

## Пропускная способность против Полосы пропускания

Беспроводная связь обычно осуществляется в пределах жестко ограниченного набора частот, называемых *полоса частот* [frequency band]. Эта полоса частот и есть *полоса пропускания* или *ширина полосы пропускания* [bandwidth]. Частотная полоса пропускания играет свою роль в итоговой пропускной способности данных, но множество других факторов также определяют пропускную способность. В дополнение к ширине полосы частот, кодирование данных, модуляция, борьба за доступ к среде, шифрование, и много других факторов также играют большую роль в пропускной способности данных.

Следует соблюдать осторожность, чтобы не путать ширину полосы частот [frequency bandwidth] и полосу пропускания данных [data bandwidth]. Кодирование данных и модуляция определяют скорость передачи данных, которая иногда называется, как полоса пропускания данных. Просто взгляните на 5ГГц каналы и OFDM, как пример. Устаревшие OFDM 802.11a радиомодули могут передавать на 6, 9, 12, 18, 24, 36, 48, или 54 Мбит/с. Однако, полоса частот 20МГц одна и та же для всех 5ГГц каналов несмотря на разные скорости. Что меняется у всех этих скоростей (передачи данных) - это модуляция и способ кодирования. Правильный термин для изменения в скорости из-за модуляции и кодирования - это *скорость передачи данных* (*data rates*); однако, часто называется, как *полоса пропускания данных* [*data bandwidth*].

Один из фактов, вызывающих удивление, при объяснении беспроводных сетей неспециалисту это реальная пропускная способность, которую предоставляют беспроводные сети 802.11. Когда новички идут по компьютерному магазину и видят упаковки Wi-Fi устройств, они скорее всего считают, что устройство, которое имеет ярлык 300 Мбит/с, предоставит им пропускную способность 300Мбит/с. Доступ к среде, называемый Множественный Доступ с Контролем Несущей и Предотвращением Конфликтов (CSMA/CA) пытается гарантировать, что только одно радиоустройство может передавать в эфир в любое выбранное время. Вы узнаете о CSMA/CA в Главе

Из-за полудуплексной природы среды и дополнительной служебной информации [overhead], создаваемой CSMA/CA, реальная агрегированная пропускная способность обычно составляет 50 процентов или меньше скорости передачи данных для устаревших передач 802.11a/b/g, и 60-70 процентов от передачи данных для передач 802.11n/ac. Однако, эти цифры основаны на чистой радиосреде и лабораторных условиях. Следовательно, хорошее предположение должно быть о том, что агрегированная пропускная способность - это около половины от рекламируемой скорости передачи данных.

Очень важно понимать, что радиосреда 802.11 является *общей* [shared] средой, означающей, что при любом обсуждении пропускной способности нужно подразумевать *агрегированную пропускную способность* [*aggregate throughput*]. Например, если скорость передачи данных 54 Мбит/с, то из-за CSMA/CA, агрегированная пропускная способность может быть около 20Мбит/с. Если пять клиентских станций загружают один и тот же файл с FTP сервера в одно и то же время, то получаемая пропускная способность для каждой клиентской станции будет около 4 Мбит/с в идеальных условиях.

RTS/CTS (о которых вы узнаете в Главе 9 "802.11 MAC") также может влиять на пропускную способность, добавляя дополнительную служебную информацию.

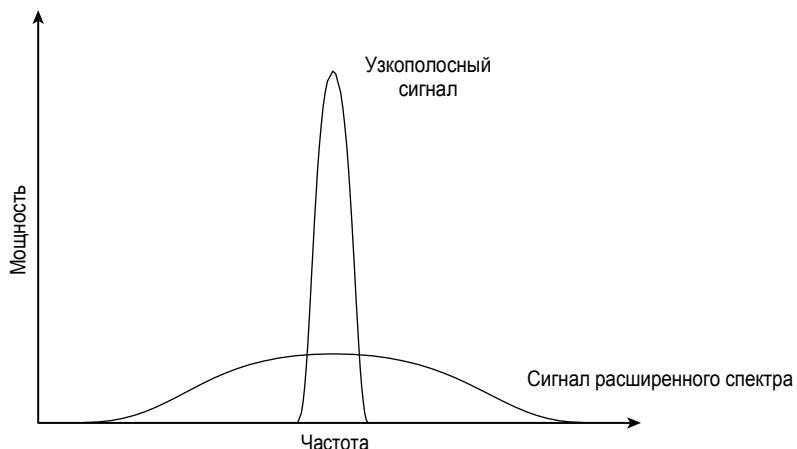
Параметры почти на всех уровнях модели OSI могут влиять на пропускную способность связи стандарта 802.11. Важно понимать разные причины, их эффекты, и что делать, если что-либо может быть сделано, чтобы минимизировать их эффект на общую пропускную способность передачи данных. В Главе 13 "Концепции Проектирования БЛВС" вы узнаете о проектировании емкости и других параметров, которые влияют на пропускную способность.

## Узкополосный сигнал и Расширение Спектра

Существует два метода радиоволновой передачи: *узкополосная передача* [*narrowband*] и *расширение спектра* [*spread spectrum*]. Узкополосная передача использует очень маленькую полосу, чтобы передать данные, в то время как расширение спектра использует большую полосу, чем необходимо, чтобы передать данные. Технология расширения спектра распределяет ("размазывает") данные, которые нужно передать, по всем частотам, которые используются. Например, узкополосный радиосигнал может передать данные в полосе 2 МГц, в то время как радиосигнал расширенного спектра может передать данные через 20МГц полосу. Рисунок 6.1 показывает упрощенное сравнение как узкополосный сигнал и сигнал с расширением спектра соотносятся друг с другом. Так как узкополосные сигналы занимают одну частоту или очень узкую полосу частот, то намеренные помехи или непреднамеренная интерференция в этом частотном диапазоне скорее всего вызовет прерывание сигнала. Так как расширенный спектр использует более широкий диапазон частот, то обычно он менее чувствителен к преднамеренным помехам или непреднамеренной интерференции от внешних источников, пока мешающий сигнал не распределится также по всему диапазону частот, используемых расширенным спектром для связи.

**Р И С У Н О К 6.1**

Наложение узкополосного сигнала на расширенный частотный спектр



Узкополосные сигналы обычно передаются с использованием намного большей мощности, чем сигналы расширенного спектра. Обычно, FCC или другие локальные регулирующие организации требуют, чтобы узкополосные передатчики получали разрешение, чтобы минимизировать риск интерференции двух узкополосных передатчиков друг на друга. АМ и FM радиостанции являются примерами узкополосных передатчиков, которые должны получать разрешения, чтобы гарантировать, что две станции в одном или соседнем районах не передают на одной и той же частоте.

Сигналы расширенного спектра передаются, используя очень низкие уровни мощности.



### Реальный Сценарий

#### Кто Изобрел Расширение Спектра?

Расширение спектра изначально было запатентовано 11 Августа 1942 года актрисой Хеди Кислер Марки (Хеди Ламар) и композитором Джорджем Антейлом. Он изначально был разработан для системы радионаведения торпед, но по назначению разработки никогда не использовалось. Идея расширения спектра была слишком передовой для своего времени. Так было до 1957 года, когда снова начали работать над расширением спектра, и в 1962 году расширение спектра со скачкообразным перестроением частоты (FHSS) было впервые применено между кораблями США при блокаде Кубы во время Кубинского Ракетного Кризиса.

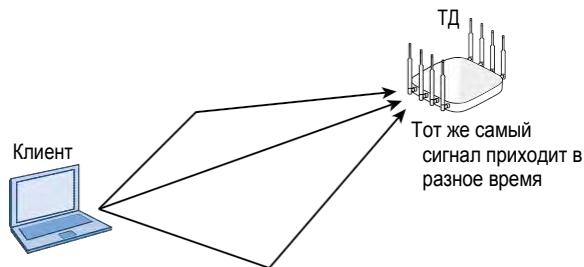
Если вы хотите узнать больше об интересной истории расширения спектра, поищите в Интернете Ламар и Антейл. Есть много вебсайтов со статьями об этих двух изобретателях и даже копии оригинального патента. Изобретатели не получили никаких денег за свой патент, так как он устарел раньше чем была разработана технология.

## Интерференция Многолучевого Распространения

Одна из проблем, которая может произойти с радиосвязью - это интерференция от *многолучевого распространения [multipath]*. Многолучевое распространение происходит, когда отраженный сигнал прибывает на приемную антенну следом за основным сигналом. Рисунок 6.2 иллюстрирует сигнал, идущий от клиента до точки доступа. В этой иллюстрации можно увидеть три различные копии одного и того же сигнала, идущих разными путями разной длины и разной длительности. Это аналогично тому как мы слышим эхо после исходного звука.

РИСУНОК 6.2

Диаграмма многолучевого распространения



Чтобы более детально продемонстрировать многолучевое распространение, давайте используем пример окрика друзей через каньон. Допустим, что вы собрались крикнуть "Привет, как дела?" вашему другу. Чтобы гарантировать, что ваш друг понимает ваше сообщение, вы разбили ваше сообщение и кричите каждое слово по отдельности через секунду после предыдущего слова.

Если ваш друг слышит эхо (многолучевое отражение вашего голоса) после полусекундной задержки после прибытия основного звука, то ваш друг услышит "ПРИВЕТ привет КАК как ДЕЛА дела." (Эхо представлено строчными буквами). Ваш друг сможет понять ваше сообщение, так как эхо приходит между основными сигналами, или звуком вашего голоса. Однако, если эхо приходит спустя секунду после основного звука, то эхо для слова *привет* придет в то же время, когда приходит слово *КАК*. Когда оба звука приходят в одно и то же время, может быть сложно понять сообщение. В результате, вашему другу может понадобится попросить вас повторить сообщение.

Радиосвязь ведет себя таким же образом, как и звук в примере. На приемнике, задержка между основным сигналом и переотраженным сигналом называется *разбросом задержки [delay spread]*. Типовой разброс задержки внутри помещений может варьироваться от 30 до 270 наносекунд (нс). Если разброс задержки слишком велик, данные от переотраженного сигнала могут интерферировать с тем же самым потоком данных от основного сигнала, это называется *межсимвольная интерференция [intersymbol interference (ISI)]*. Системы расширения спектра не восприимчивы к межсимвольной интерференции, потому что они распределяют свои сигналы по всему диапазону частот. Эти различные частоты дают разную задержку при многолучевом распространении, так что некоторые длины волн могут быть подвержены влиянию межсимвольной интерференции, в то время как другие нет. Из-за такого поведения сигналы расширенного спектра обычно являются более толерантными к интерференции многолучевого распространения, чем узкополосные сигналы.

Технологии 802.11 такие как 802.11 (DSSS), 802.11b (HR-DSSS), и 802.11g (ERP) толерантны к разбросу задержки только в определенной степени. Даже если разброс задержки допустим, производительность намного лучше, когда разброс задержки меньше. Передатчик будет переходить на меньшую скорость передачи при увеличении разброса задержки. Более длинные символы используются при меньших скоростях передачи данных. Когда используются длинные символы, могут появится более длинные задержки прежде появления межсимвольной интерференции (ISI).

Так как OFDM значительно терпимее к разбросу задержке, передатчики 802.11a/g могут поддерживать 54Мбит/с с разбросом задержки вплоть до 150 наносекунд. Это зависит от микросхемы/чипсета [chipset] 802.11a/g, которая используется в передатчике и приемнике. Некоторые чипсеты не толерантны и переключаются на более низкую скорость передачи данных при более высоком значении разброса задержки.

До технологии MIMO 802.11n и 802.11ac, многолучевое распространение всегда было проблемой. Это было явление, которое могло радикально повлиять на производительность и пропускную способность беспроводной ЛВС. С появлением MIMO, многолучевое распространение является реальным явлением, которое улучшает и увеличивает производительность беспроводной ЛВС.

Улучшенные методы цифровой обработки сигналов устройств MIMO используют преимущества одновременной множественной передачи и может действительно извлечь выгоду из эффекта многолучевого распространения. Вы узнаете больше о 802.11n/ac и MIMO в Главе 10, "Технология MIMO: HT и VHT".

## Расширение спектра со скачкообразной перестройкой частоты

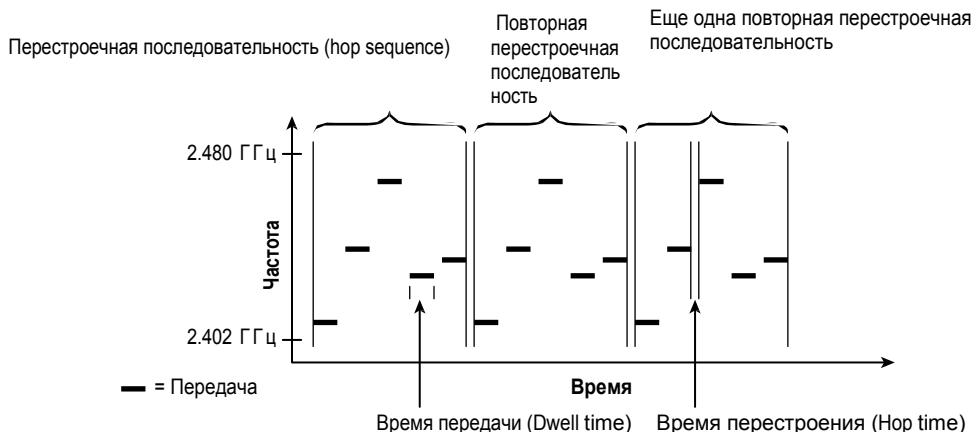
*Расширение спектра со скачкообразной перестройкой частоты [Frequency-hopping spread spectrum (FHSS)]* использовалось в изначальном стандарте 802.11 и обеспечивало 1Мбит/с и 2Мбит/с радиосвязь, используя полосу 2,4ГГц ISM для старых радиоустройств. Основная масса старых радиоустройств FHSS была произведена между 1997 и 1999 годами. IEEE определяла, что в Северной Америке, FHSS в стандарте 802.11 будет использовать полосу частот 79 МГц от 2,402ГГц до 2,480 ГГц.



Стандарт IEEE 802.11-2020 упразднил FHSS, полностью убрав его из действующего документа. Технология 802.11 FHSS не будет проверяться на экзамене CWNA. Производители 802.11 устройств перестали выпускать адAPTERЫ и точки доступа с FHSS уже давным-давно. Большинство организаций уже давно перешли с 802.11 FHSS на один из более новых и быстрых методов передачи. Но все еще важно понимать основы FHSS, поскольку существуют и другие технологии, такие как Bluetooth, которые используют FHSS. Знайте, что хоть Bluetooth и

В общем, метод работы FHSS заключается в том, что он передает данные, используя небольшое пространство несущей частоты, затем перестраивается(перепрыгивает) на другое небольшое пространство несущей частоты и передает данные, затем на другую частоту, и так далее, как показано на Рисунке 6.3. Более точно, FHSS передает данные используя определенную частоту определенный период времени, называемый *время передачи или время жизни [dwell time]*. Когда время передачи выходит, система переходит на другую частоту и начинает передачу на этой частоте продолжительностью равной времени передачи. Каждый раз, когда достигается время передачи, система переходит на другую частоту и продолжает передавать.

**Р И С У Н О К 6 . 3** Состав FHSS



## Перестроечная последовательность

Радиомодули FHSS используют предопределенную перестроечную последовательность [*hopping sequence*] (также называемую как *шаблон перестройки частоты [hopping pattern]* или *набор перестроичных частот [hopping set]*), содержащую серию небольших несущих частот [*hops*]. Вместо передачи на одном заданном канале или конечном пространстве частот, радиомодуль FHSS передает на последовательности подканалов, что называется скачкообразным перестроением [*hops*]. Каждый раз, когда завершается последовательность перестроичных частот, она повторяется. Рисунок 6.3 показывает выдуманную перестроичную последовательность, которая состоит из пяти перестроений (скакков).

Оригинальный стандарт IEEE 802.11 указывает, что каждый скачок (перестройка частоты) будет 1МГц. Эти индивидуальные перестройки были затем упорядочены в предопределенные последовательности. В Северной Америке и большей части Европы, перестроичные последовательности содержат как минимум 75 прыжков (перестроек частоты), но не более 79. Другие страны имеют другие требования, например, Франция использует 35 перестроек частоты, а Испания и Япония используют 23 прыжка в последовательности. Для успешной передачи, все FHSS передатчики и приемники должны быть синхронизованы на одну и ту же несущую частоту в одно и то же время. Первоначальный стандарт 802.11 определял, что перестроичную последовательность можно настроить на FHSS точке доступа, а информация о перестроичной последовательности доставляется клиентским станциям с помощью кадра управления маяк [*beacon*].

## Время Передачи

*Время передачи или время жизни [Dwell time]* - это определенное количество времени, которое FHSS система передает на определенной частоте, прежде чем переключиться на следующую частоту из набора перестроичных частот. Локальные регулирующие организации обычно ограничивают время передачи. Например, FCC определяет максимальное время передачи в 400 миллисекунд (мс) на несущую частоту в течении любого 30 секундного периода. Типовое время передачи где-то от 100мс до 200 мс. Первоначальный стандарт IEEE 802.11 определял, что перестроичная последовательность содержит как минимум 75 частот, шириной 1 МГц. Так как стандарт определял максимальную полосу в 79 МГц, максимальное возможное количество перестроичных частот в наборе перестроичных частот могло быть 79. Перестроичная последовательность FHSS, содержащая 75 частот с временем передачи 400 мс на каждой частоте, займет примерно 30 секунд, чтобы пройти всю последовательность. После того, как перестроичная последовательность завершена, она повторяется.

## Время перестроения

*Время перестроения или время прыжка [Hop time]* не является специфицированным периодом времени, а является параметром количества времени, которое требуется передатчику чтобы перейти с одной частоты на другую. Время перестроения обычно довольно маленькое число, чаще всего от 200 до 300 микросекунд (мкс или  $\mu$ s). По сравнению со временем передачи от 100 до 200 миллисекунд (мс), время перестроения от 200 до 300 мкс является незначительным. Незначительное или нет, но время перестроения, по сути, является потраченным впустую временем, или накладными расходами [*overhead*], и одинаково независимо от времени передачи. Чем длительнее

**226** Глава 6 • Беспроводные Сети и Технологии Расширения Спектра  
время передачи, тем реже передатчик должен впустую тратить время перестраиваясь на другую частоту, в результате увеличивая пропускную способность. Если время передачи короче, то передатчик должен перестраиваться более часто, таким образом уменьшая пропускную способность.

## Модуляция

FHSS использует Гаусову Частотную Модуляцию (GFSK) чтобы закодировать данные. Двух уровневая Гауссова Частотная Модуляция (2GFSK) использует две частоты, чтобы представить один бит со значением 0 или 1. Четырехуровневая Гауссова Частотная Модуляция (4GFSK) использует четыре частоты, представляя каждой частотой два бита (00, 01, 10, или 11). Поскольку требуются циклы передач, прежде чем частота может быть определена, символьная скорость (скорость, с которой отправляются данные) составляет только один или два миллиона символов в секунду, часть от несущей частоты 2,4ГГц.

### В чем значимость Времени Передачи?

Так как передачи FHSS прыгают внутри частотного диапазона 79 МГц, узкополосный сигнал или шум помешает только небольшому диапазону частот и создаст только минимальное количество потери пропускной способности. Уменьшение времени передачи может дальше уменьшить эффект интерференции. И наоборот, так как радиомодуль передает данные только во время передачи, чем длиннее время передачи, тем больше пропускная способность.

# Расширение спектра прямой последовательностью

*Расширение спектра прямой последовательностью [Direct-sequence spread spectrum (DSSS)]* было изначально специфицировано в основном, или корневом, стандарте 802.11 и поддерживало радиосвязь 1Мбит/с и 2Мбит/с, используя полосу ISM 2,4ГГц. Обновленная реализация DSSS (HR-DSSS) также была специфицирована в дополнении 802.11b и поддерживала радиосвязь с 5,5 и 11 Мбит/с, используя ту же полосу ISM 2,4ГГц. Скорости 5,5 и 11 Мбит/с стандарта 802.11b называются *высоко-скоростное DSSS [high-rate DSSS (HR-DSSS)]*.

Текущие устройства 2,4ГГц стандарта 802.11 обратно совместимы со старыми 802.11 DSSS устройствами. Это значит, что устройства 802.11b могут передавать, используя DSSS с 1 и 2 Мбит/с, а используя HR-DSSS с 5,5 и 11Мбит/с. И старые устройства 802.11 DSSS и 802.11b HR-DSSS считаются очень старыми технологиями (более 15 лет). Однако, это не является не обычным для клиентских устройств 802.11b все еще иногда существовать среди клиентских устройств на предприятиях.



DSSS 1 и 2 Mbps специфицированы в Статье 15 стандарта 802.11-2020.  
HR-DSSS 5,5 и 11 Мбит/с специфицированы в Статье 16 стандарта 802.11-2020.

В отличие от FHSS, где передатчик прыгает между частотами, DSSS установлен на одном канале. Передаваемые данные распределяются по всему диапазону частот, из которых состоит канал. Процесс распределения данных по каналу называется *кодирование данных [data encoding]*.

## Кодирование данных при DSSS

В Главе 3 “Основы Радиотехники” вы узнали о многих вариантах, при которых радиосигналы могут подвергнуться изменению или повредиться. Поскольку радиосвязь 802.11 использует неограниченную среду с большим потенциалом к радио-интерференции, оно должно быть спроектировано, чтобы быть достаточно устойчивым, чтобы можно было бы минимизировать повреждение данных. Чтобы достичь этого, каждый бит данных кодируется и передается как несколько битов данных.

Задача добавления дополнительной, резервной информации к данным называется *усилением обработки [processing gain]*. В наши дни, эпохи сжатия данных, кажется странным, что мы собираемся использовать технологию, которая добавляет данные к нашей передаче, но, когда мы так делаем, связь более устойчива к повреждению данных. Система конвертирует 1 бит данных в серию битов, которые называются *элементами или чипами (chips*, в переводе с англ. - кусочки.). Чтобы создать элементы [chips], производится Булевая операция XOR с битами данных и псевдослучайным числовым [(pseudorandom number (PN)] кодом фиксированной длины. Используя псевдослучайный числовой код, который называется код Баркера, двоичные данные 1 и 0 представляются следующим последовательностями элементов (чипов):

Двоичные данные 1 = 1 0 1 1 0 1 1 1 0 0 0

Двоичные данные 0 = 0 1 0 0 1 0 0 0 1 1 1

Эта последовательность элементов-чипов затем распределяется по широкому частотному пространству. Хотя 1 биту данных может требоваться 2Мгц частотного пространства, 11 элементов-чипов потребуют 22 Мгц пространства несущей частоты. Этот процесс конвертирования единичных битов данных в последовательность часто называется *расширение [spreading]* или разбиение [*chipping*]. Приемный радиомодуль конвертирует, или проводит обратную операцию расширению [*de-spreading*], последовательность элементов(чипов) обратно в единичный бит данных. Когда данные преобразованы в несколько элементов(чипов), а некоторые из элементов(чипов) приняты неправильно, радиомодуль все-равно сможет распознать данные путем просмотра элементов(чипов), которые были приняты правильно. При использовании кодов Баркера, 9 из 11 элементов(чипов) могут быть повреждены, а приемный радио модуль будет все еще способен распознавать последовательность и преобразовывать ее обратно в единичный бит данных. Этот процесс расширения также делает менее вероятным влияние межсимвольной интерференции на связь, потому что он использует большую полосу.



После применения кода Баркера к данным, серия из 11 битов, называемых элементами(чипами), представляет исходный единичный бит данных. Эта серия кодовых битов составляет 1 бит данных. Чтобы помочь избежать путаницы, лучше всего называть кодовые биты элементами(чипами).

Код Баркера использует 11 элементное (11 чиповое) псевдослучайное число; однако, длина кода не имеет значения. Чтобы помочь обеспечить более высокие скорости в HR-DSSS, используется другой более сложный код - *кодирование комплиментарными кодами [complementary code keying (CCK)]*. CCK использует 8-элементное (8 чиповое) псевдослучайное число, вместе с различными псевдослучайными числами для различных битовых последовательностей. CCK может закодировать 4 бита данных 8ю элементами(чипами) (5,5Мбит/с), м может закодировать 8 бит данных с помощью 8 элементов(чипов) (11 Мбит/с). Хоть это и интересно знать, полное понимание CCK не требуется для экзамена CWNA.

## Модуляция

После того, как данные закодированы с использованием метода разбиения [*chipping*], передатчику нужно промодулировать сигнал, чтобы создать несущий сигнал, состоящий из элементов(чипов). *Дифференциальная двоичная фазовая манипуляция [Differential binary phase-shift keying (DBPSK)]* использует два изменения фазы (или фазовые смены): одно изменение представляет элемент(чип) с значением 0, а другое, представляет элемент(чип) со значением 1. Чтобы обеспечить более скоростную пропускную способность, *дифференциальная квадратурная фазовая манипуляция (differential quadrature phase-shift keying (DQPSK))* использует четыре смены фазы, позволяя каждой из четырех смен фазы модулировать 2 элемента(чипа) (00, 01, 10, 11) вместо 1, удваивая скорость.

Таблица 6.1 показывает сводную информацию о кодировании данных и способах модуляции используемых старыми радиомодулями 802.11 и 802.11b.

ТАБЛИЦА 6.1

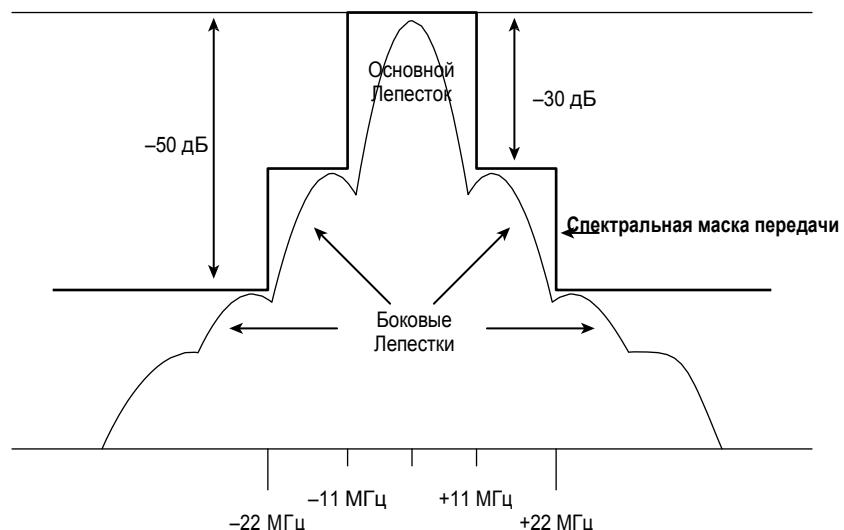
	Скорость передачи данных (Мбит/с)	Кодирование	Длина кодовой последовательности	Количество кодируемых битов	Модуляция
DSSS	1	Кодирование Баркера	11	1	DBPSK
DSSS	2	Кодирование Баркера	11	1	DQPSK
HR-DSSS	5.5	Кодирование CCK	8	4	DQPSK
HR-DSSS	11	Кодирование CCK	8	8	DQPSK

## Спектральная Маска Передачи

Хоть это очень распространено - изображать радиосигнал определенного канала линией в виде арки, это неверное представление сигнала. *Спектральная маска передачи* [*transmit spectrum mask*], также называется просто *спектральная маска* [*spectral mask*], используется, чтобы определить ограничения спектральной плотности передачи 802.11 БЛВС. Иногда спектральной маской называют форму канала. Вместо этого, постарайтесь думать о спектральной маске как о частотной ширине, в которой мощность сигнала должна уменьшиться на определенное количество. Цель - минимизировать интерференцию с соседними каналами и соседними полосами частот. Накладываются ограничения как по мощности, так и по ширине частоты.

Например, в дополнение к основной *несущей частоте* [*carrier frequency*], или главной частоте, создаются боковые несущие частоты, как показано на Рисунке 6.4. В этом примере, IEEE определяет спектральную маску передачи для 22МГц канала HR-DSSS. Первые боковые частоты (от -11МГц до -22МГц от центральной частоты и от +11 МГц до +22МГц от центральной частоты) должны быть меньше хотя бы на 30дБ чем основная частота. Мaska также определяет, что любые дополнительные боковые несущие частоты (от -22 МГц от центральной частоты и далее и от +22 МГц от центральной частоты и далее), должны быть меньше хотя бы на 50дБ по сравнению с основной частотой.

**Р И С У Н О К 6 . 4** Спектральная маска передачи HR-DSSS

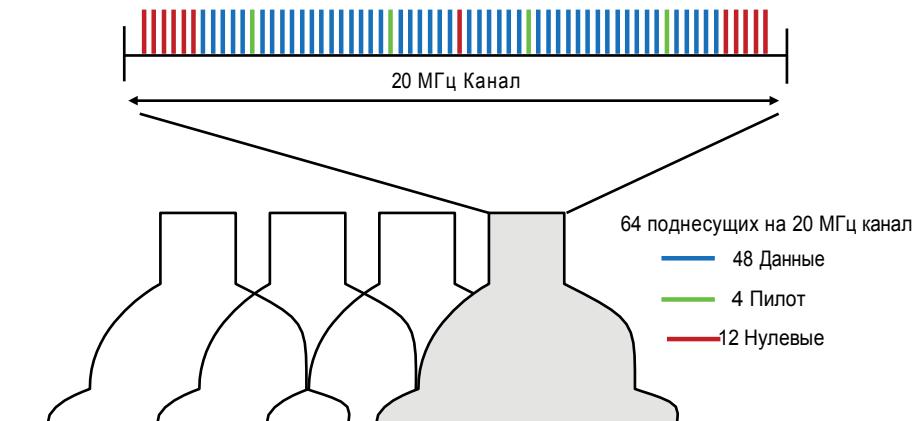


Как упоминалось, спектральная маска передачи определена, чтобы минимизировать интерференцию между устройствами на разных частотах. Даже если боковые несущие частоты - это всего лишь шепот сигнала, по сравнению с основной несущей частотой, но даже шепот заметен, когда кто-нибудь шепчет рядом с вами. Это верно и для радиоустройств тоже.

# Мультиплексирование с Ортогональным Частотным Разделением

*Мультиплексирование с Ортогональным Частотным Разделением [Orthogonal frequency-division multiplexing (OFDM)]* является одной из наиболее популярных технологий связи, используемой как в проводной, так и беспроводной связи. Стандарт 802.11-2020 определяет использование OFDM на 5 ГГц и использование ERP-OFDM на 2,4 ГГц. OFDM и ERP-OFDM являются одной и тоже технологией, используемой 802.11a и 802.11g радиомодулями, соответственно. OFDM - это не технология расширения спектра, даже если она имеет сходные свойства с расширением спектра, такие как низкая мощность передачи и использование большей полосы, чем требуется, для передачи данных. Из-за этих сходств, OFDM часто называют технологией расширения спектра, хотя технически такое название некорректно. 20 МГц OFDM канал состоит из 64 отдельных и точно расположенных частотами с промежутками между ними, часто называемых *поднесущими* [*subcarriers*], как показано на Рисунке 6.5. Поднесущие OFDM иногда также называют как *тоны* [*tones*] OFDM.

**РИСУНОК 6.5** Каналы 802.11a/g и поднесущие OFDM



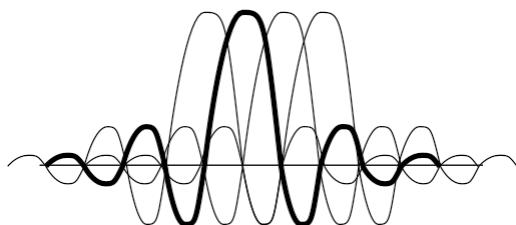
Двенадцать из 64 поднесущих в 20МГц OFDM канале не используются и служат в качестве защитных интервалов (полос). *Защитная полоса* [*guard band*] - это неиспользуемая часть радиоспектра между радио полосами, с целью предотвращения интерференции. Сорок восемь поднесущих используются для передачи модулированных данных. Еще четыре поднесущих называются, как *пилотные насыщие* [*pilot carriers*], и используются для динамической калибровки между передатчиком и приемником. Эти четыре пилотных тона используются демодулятором в качестве опорного сигнала для фазы и амплитуды, позволяя приемнику синхронизоваться, когда он демодулирует данные из других поднесущих.

Ширина частоты каждой поднесущей 312,5 кГц. Поднесущие тоже передают на более низких скоростях передачи данных, но суммарная скорость передачи данных выше. Также, из-за более низких скоростей передачи данных поднесущих, разброс задержки составляет небольшой процент от времени длительности символа, что означает, что мало вероятно, что случиться межсимвольная интерференция (ISI). Другими словами, технология OFDM более устойчива к негативным эффектам многолучевого распространения, чем технологии расширения спектра DSSS и FHSS. Рисунок 6.6 показывает четыре поднесущих. Одна из поднесущих выделена так, что вы можете более просто понять рисунок. Заметьте, что расстояние между частотами поднесущих выбрано так, чтобы гармоники перекрывались и обеспечивали гашение большей части ненужных сигналов. Расположение поднесущих является ортогональным, так что они не интерферируют друг с другом. Время символа в OFDM равно 3,2 (мкс или  $\mu$ s). Расстояние между поднесущими равно обратной величине времени символа OFDM. Например:

$$1 \text{ цикл}/0.00000032 = 312,500 \text{ циклов в секунду} = 312.5 \text{ кГц.}$$

#### Р И С У Н О К 6.6

Наложение поднесущих сигналов



В Главе 10, вы узнаете, что радиомодули 802.11n/ac также используют OFDM технологию.

Радиомодули 802.11n/ac также передают на каналах в 20МГц, которые состоят из 64 поднесущих, хотя только 8 поднесущих являются защитными интервалами. Пятьдесят две поднесущих используются для передачи модулированных данных, а четыре поднесущих работают в качестве несущих пилотных сигналов.

## Сверточное кодирование

Чтобы сделать OFDM более устойчивым к узкополосной интерференции, применяется форма коррекции ошибок, называемая как *сврточное кодирование* [*convolutional coding*]. Стандарт 802.11-2020 определяет использование сврточного кодирования как способ коррекции ошибок для использования с технологией OFDM.

Это *прямая коррекция ошибок* [*forward error correction (FEC)*], которая позволяет приемной системе обнаружить и восстановить поврежденные биты.

Существует много уровней сврточного кодирования. Сврточное кодирование использует соотношение между переданными битами и закодированными битами, чтобы обеспечить эти различные уровни. Чем меньше отношение, тем меньше устойчивость сигнала к интерференции и тем больше будет скорость передачи данных. Таблица 6.2 показывает сравнение между технологиями, используемыми чтобы создать

различные скорости передачи данных для 802.11a и 802.11g. Заметьте, что скорости передачи данных сгруппированы попарно на основе способа модуляции, и что разница между двумя скоростями вызвана различными уровнями сверточного кодирования.

Детальное объяснение сверточного кодирования черезвычайно сложное и далеко за пределами знаний, необходимых для экзамена CWNA.

**ТАБЛИЦА 6.2** Сравнение скоростей передачи данных и модуляций 802.11a и 802.11g

Скорость передачи данных (Мбит/с)	Модуляция	Закодированные биты на поднесущую	Биты данных на OFDM символ	Закодированные биты на OFDM символ	Скорость кодирования (биты данных / закодированные биты)
6	BPSK	1	24	48	1/2
9	BPSK	1	36	48	3/4
12	QPSK	2	48	96	1/2
18	QPSK	2	72	96	3/4
24	16-QAM	4	96	192	1/2
36	16-QAM	4	144	192	3/4
48	64-QAM	6	192	288	2/3
54	64-QAM	6	216	288	3/4

## Модуляция

OFDM использует двоичную фазовую манипуляцию (BPSK) и квадратурную фазовую манипуляцию (QPSK) для более низких скоростей передачи данных. Более высокие скорости передачи данных OFDM используют модуляции 16-QAM, 64-QAM, и 256-QAM. *Квадратурная Амплитудная Модуляция [Quadrature amplitude modulation (QAM)]* объединяет и фазовую и амплитудную модуляцию. *Диаграмма созвездий [constellation diagram]*, еще называемая картой созвездий, двухмерная диаграмма, часто используемая для представления модуляции QAM. Диаграмма созвездий делится на четыре квадранта, а различные местоположения в каждом квадранте используются для представления битов данных.

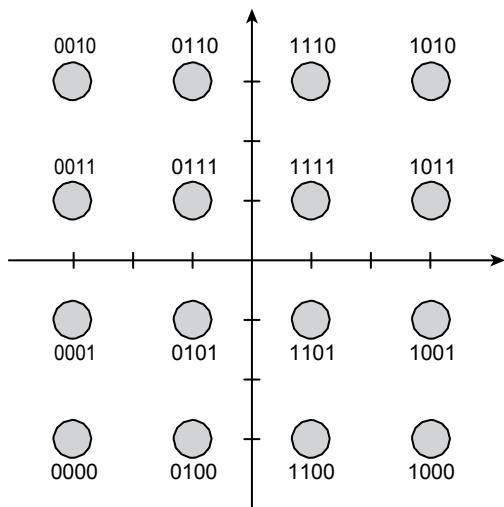
Области в квадранте относительно горизонтальной оси используются для представления разных смен фазы. На рисунке 6.7 первые два бита представляются сменой фазы. Обратите внимание, что первые два бита одни и те же в одном столбце. Области относительно вертикальной оси используются для представления смены амплитуды. В этом примере, последние 2 бита представлены сменой амплитуды. Обратите внимание, что последние два бита одни и те же в одном ряду.

Как показано в двух примерах созвездий 16-QAM на Рисунке 6.8, угол точки измеряемый против часовой стрелки от горизонтальной оси, представляет смену фазы несущей волны от фазы опорного сигнала. Расстояние точки от начала координат представляет собой меру амплитуды или мощности сигнала. Левое созвездие изображает фазу 225 градусов в третьем квадранте, совмещенную с 25 процентным

уровнем амплитуды, и представляет биты данных 0101. Правое созвездие изображает фазу 337 градусов в четвертом квадранте, совмещенную с 75 процентами от уровня амплитуды, и представляющие биты данных 1001.

Р И С У Н О К 6 . 7

Диаграмма созвездий 16-QAM



Р И С У Н О К 6 . 8

Диаграмма созвездий: фаза и амплитуда

Амп	Фаза	Данные
25%	225%	0101

Амп	Фаза	Данные
5%	337%	1001

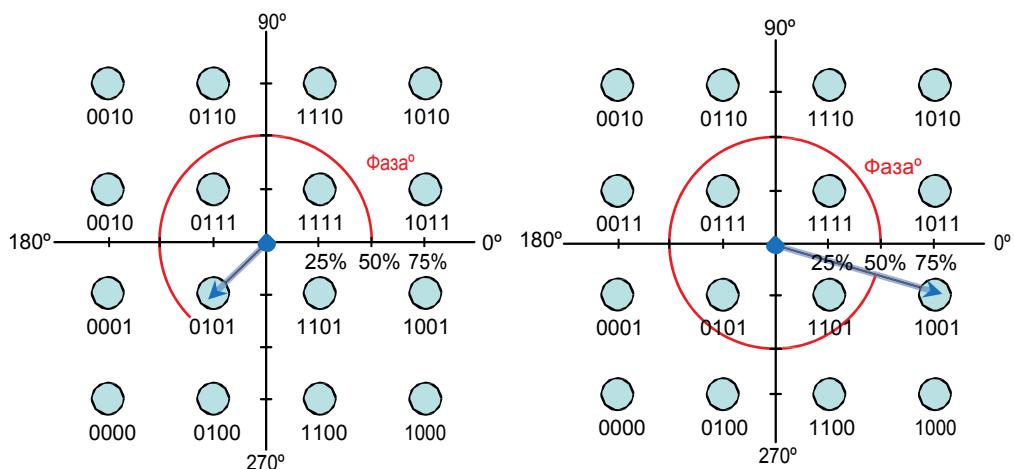
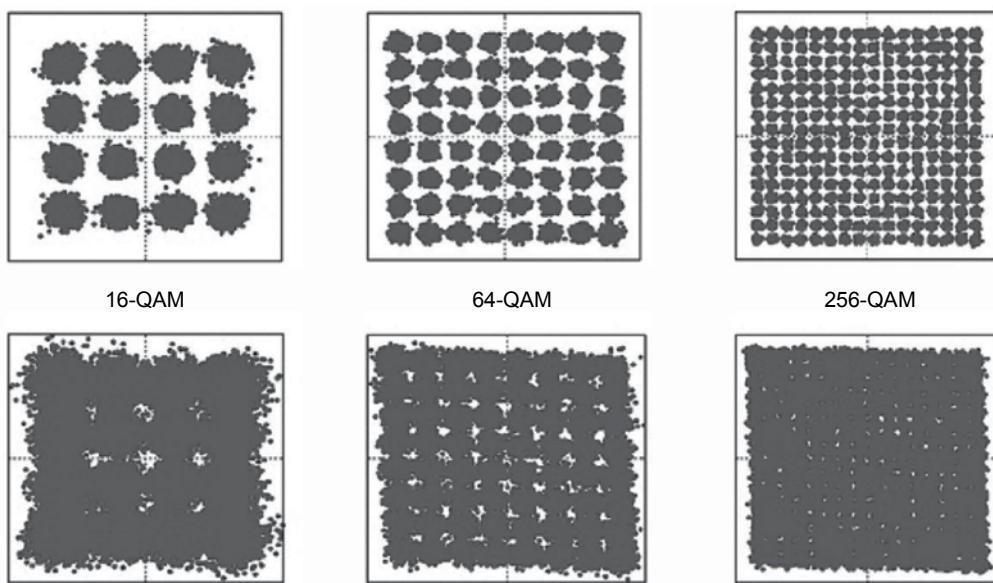


Диаграмма созвездий 16-QAM использует четыре различные смены фаз и четыре различные смены амплитуды, чтобы создать в сумме 16 четырехзначных комбинаций. Каждая из 16 различных точек в четырех квадрантах используется, чтобы представить по 4 бита данных. Глава 10 объясняет карты созвездий более детально.

*Модуль вектора ошибок [Error vector magnitude (EVM)]* - это мера, используемая для количественной оценки характеристик радиоприемника или передатчика в отношении точности модуляции. В модуляции QAM, EVM это мера того, как далек полученный сигнал от идеального местоположения в созвездии. Другой вариант объяснения, EVM - это мера того как сильно точки созвездия сигнала отклоняются от идеального местоположения. Если отклонение слишком велико, то страдает точность модуляции. Высококачественные радиомодули имеют большую устойчивость к отклонениям. Для измерения EVM передатчика можно использовать дорогое измерительное оборудование. Рисунок 6.9 изображает хорошую и слабую точность модуля вектора амплитуды (EVM) для модуляций 16-QAM, 64-QAM и 256-QAM. Верхний ряд изображает более высокую точность EVM. Чем более сложная модуляция QAM, тем меньше места для точности. Радио среда также может повлиять на точность модуляции, вот почему нужны чистая радиостанция и отношение сигнал-шум (SNR) в 35дБ или лучше для радиомодулей 802.11ax, чтобы использовать модуляцию 1024-QAM.

**Р И С У Н О К 6 . 9** Модуль вектора ошибок

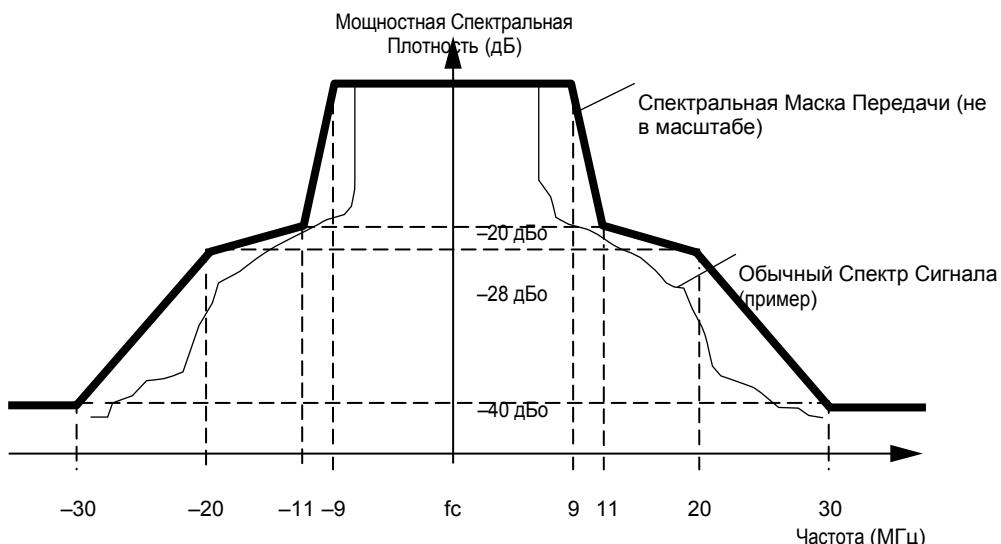


## Спектральная Маска передачи

Спектральная маска передачи OFDM используемая радиомодулями 802.11a/g/n/ac/ax выглядит совершенно по-другому нежели спектральная маска HR-DSSS, используемая радиомодулями 802.11b. Как утверждалось ранее, IEEE специально не определяет ширину канала, однако, спектральная маска канала OFDM примерно 20МГц.

Как вы можете видеть на Рисунке 6.10, 20МГц Спектральная маска и форма OFDM канала очень отличаются.

**Р И С У Н О К 6.10** Спектральная маска передачи OFDM (20МГц канал)

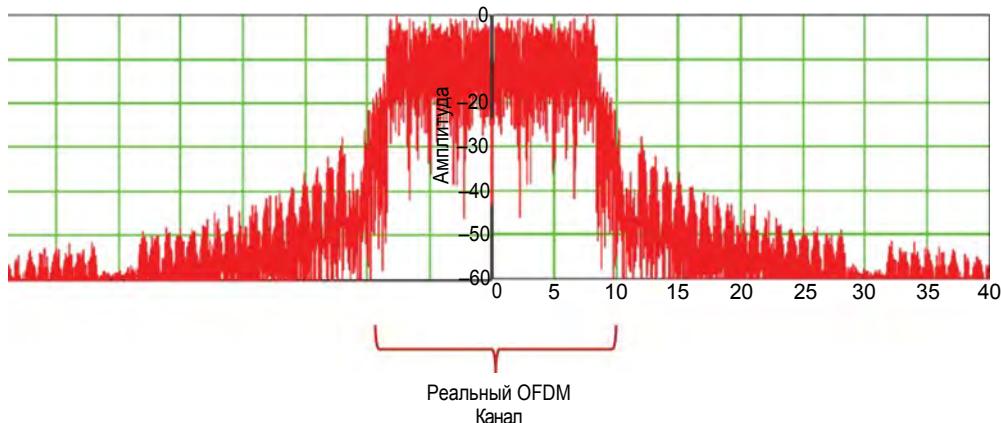
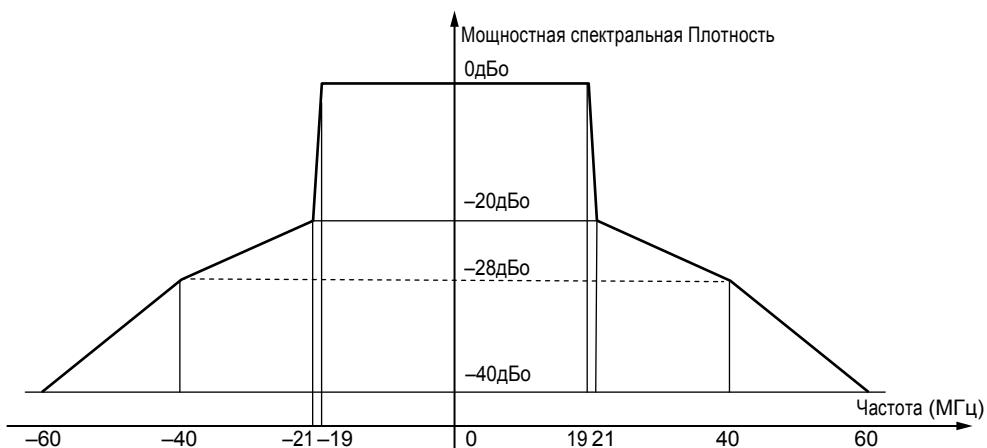


Большинство диаграмм спектральной маски передачи использует размерность дБо (dB<sub>r</sub>), чтобы определить силу сигнала. Вспоминаем, что децибел (dB) - это мера изменения мощности. дБо (dB<sub>r</sub>) это количество децибел относительно опорного уровня. Следовательно, дБо (dB<sub>r</sub>) это мера изменения мощности относительно определенного опорного уровня. Опорный уровень в диаграмме маски передачи - это *максимальная спектральная плотность [maximum spectral density]* радиосигнала.

Для 20МГц OFDM канала, спектральная маска передачи определяет -20дБо на 11МГц частотных сдвигах, и -28дБо на 20Мгц сдвигах от опорной максимальной спектральной плотности сигнала. Спектральная маска слегка отличается между 20МГц OFDM каналами на 2,4ГГц и 5 ГГц полосами. Уровни дБо поднесущих на сдвигах 30Мгц -45дБо для 2,4ГГц канала и -40дБо для 5ГГц канала. Как показано на Рисунке 6.11, спектроанализатор визуализирует спектральную маску 20Мгц OFDM канала.

В Главе 10, вы узнаете о 40Мгц каналах, используемых радиомодулями 802.11n/ac/ax. Сорокамегагерцовые каналы по существу являются двумя 20МГц OFDM каналами, которые объединены вместе. Как изображено на Рисунке 6.12, спектральная маска 40Мгц выглядит идентично маске 20Мгц, кроме того, что она вдвое шире.

Для 40Мгц OFDM канала, спектральная маска передачи определяет -20дБо на сдвиге 21 МГц по частоте, и -28дБо на 40Мгц сдвиге от опорной максимальной спектральной плотности сигнала.

**Р И С У Н О К 6.11** Вид на спектроанализаторе: 20 Мгц OFDM канал**Р И С У Н О К 6.12** Спектральная маска передачи OFDM (40 МГц канал)

## Множественный Доступ с Ортогональным Частотным Разделением

*Множественный доступ с Ортогональным Частотным Разделением [Orthogonal frequency-division multiple access (OFDMA)]* - это многопользовательская версия технологии OFDM. Радиомодули 802.11a/g/n/ac в настоящее время используют мультиплексирование с ортогональным частотным разделением (OFDM) для однопользовательской передачи на частоте технологии 802.11. OFDMA делит канал на небольшие частотные блоки, называемые *ресурсными блоками* [*resource units (RUs)*]. Путем разделения канала, может одновременно происходить параллельная передача небольших кадров для нескольких пользователей. Думайте об OFDMA как о технологии, которая разбивает канал на небольшие подканалы, так чтобы могла происходить одновременно многопользовательская передача.

Например, традиционный 20МГц канал может быть разделен на четыре меньших канала. Каждый меньший подканал будет состоять из набора OFDM поднесущих из оригинального 20Мгц канала. Технология OFDMA используется для сотовой связи уже много лет, и теперь используется Wi-Fi радиомодулями 802.11ax. Подробное объяснение OFDMA можно найти в Главе 19, "802.11ax: Высокая Эффективность".

## Промышленные, Научные и Медицинские Полосы Частот

Изначальный стандарт 802.11 и последующие поправки 802.11b, 802.11g, и 802.11n, все определяют связь в частотном диапазоне между 2,4ГГц и 2,4835 ГГц. Этот частотный диапазон - один из трех частотных диапазонов, которые называются *промышленные, научные и медицинские полосы [industrial, scientific, and medical (ISM) bands]*. Частотные диапазоны Промышленных, Научных и Медицинских (ISM) полос:

- 902 МГц - 928 МГц (ширина 26 МГц)
- 2.4 ГГц - 2.5 ГГц (ширина 100 МГц)
- 5.725 ГГц - 5.875 ГГц (ширина 150 МГц)

Полосы ISM определены Отделом Стандартизации Телекоммуникаций ITU (ITU-T) в S5.138 и S5.150 Радио Регламента. Хотя FCC управляет использованием полос ISM, определенным ITU-T в Соединенных Штатах, их использование в других странах может быть другим из-за локального регулирования. Полоса 900 МГц называется промышленная полоса, полоса 2,4ГГц - называется научной полосой, и полоса 5,8ГГц называется медицинской полосой.

Заметьте, что все три из этих полос являются полосами, не требующими разрешений, и нет ограничений по типу используемого оборудования в любом из них. Например, радио, используемое в медицинском оборудовании может использоваться в промышленном диапазоне 900 Мгц.

\* В России полоса 900МГц выделена для подвижной, радионавигационной связи. Для устройств с малым радиусом действия, рекомендована для локаторов (измерителей) нелинейности.

### Полоса ISM 900 МГц

Полоса 900 МГц ISM 26МГц ширины и находится от 902МГц до 928МГц. В прошлом, эта полоса использовалась для беспроводных сетей, однако, большинство беспроводных сетей теперь используют более высокие частоты, которые предоставляют большую полосу частот для модуляции данных.

Еще один фактор, ограничивающий использование полосы 900МГц ISM, это то, что во многих частях Земного Шара часть частотного диапазона 900Мгц уже выделена Глобальной Системе Мобильной Связи [Global System for Mobile Communications (GSM)] для использования мобильными телефонами. Хотя полоса 900 МГц ISM редко используется для сетей, многие продукты, такие как радионяни, беспроводные домашние телефоны, и беспроводные наушники используют этот частотный диапазон.

Радиомодули 802.11 не работают в полосе 900 МГц ISM, но многие старые установки беспроводных сетей работали в этом диапазоне. Некоторые производители все еще выпускают не-802.11 устройства беспроводных сетей, которые работают в полосе 900 МГц ISM.

Это особенно популярная частота, которая используется беспроводными провайдерами (ISP) из-за ее превосходного проникновения сквозь листву по сравнению с диапазонами частот 2,5ГГц и 5ГГц.

## Полоса ISM 2.4 ГГц

Полоса 2,4ГГц ISM исторически самая привычная полоса, используемая для беспроводной сетевой связи. Полоса 2.4 ГГц ISM 100 МГц ширины и распространяется от 2,4ГГц до 2,5ГГц. Использование 2,4ГГц ISM для беспроводных ЛВС определено IEEE в стандарте 802.11-2020. С большинством текущих радио микросхем 802.11 включающими теперь и поддержку 5ГГц, использование полосы 2,4ГГц ISM уменьшилось, хотя полоса 2,4ГГц все еще чрезвычайно переполнены.

Следующие радиотехнологии 802.11 передают в этой полосе:

- 802.11 (FHSS или DSSS)
- 802.11b (HR-DSSS )
- 802.11g (ERP)
- 802.11n (HT)
- 802.11ax (HE)

В дополнение к использованию оборудованием БЛВС 802.11, полоса 2,4ГГц ISM используется микроволновыми печами, беспроводными домашними телефонами, радио-нянями и беспроводными видеокамерами. Другие радиотехнологии такие, как Bluetooth и Zigbee, также передают в полосе 2,4ГГц. Bluetooth использует передачу FHSS, а Zigbee использует передачу DSSS. Полоса ISM 2,4ГГц интенсивно используется, и один из больших недостатков использования радиомодулей 802.11b/g/n/ax 2.4 ГГц – это возможная интерференция.

Пожалуйста, держите в уме, что не каждый государственный регулирующий радио орган разрешит передачу по всей полосе от 2,4ГГц до 2,5ГГц. Стандарт IEEE 802.11-2020 разрешает передачу БЛВС в полосе по 14 каналам. Однако, каждая страна может определить какие каналы могут быть использованы. Обсуждение всех каналов 2,4ГГц будет позже в этой главе.

## Полоса ISM 5.8 ГГц

Полоса ISM 5,8 ГГц это 150МГц находящихся от 5,725ГГц до 5,875ГГц. Как и другие ISM полосы, полоса ISM 5,8ГГц используется большинством продуктов того же типа: радио-няни, беспроводные телефоны, и камеры. Не является необычным для новичков перепутать полосу ISM 5,8ГГц с полосой U-NII-3, которая простирается от 5,725ГГц до 5,85ГГц. Обе нелицензируемые полосы занимают одно и тоже частотное пространство; однако, полоса 5,8ГГц ISM на 25МГц больше.

Поправка IEEE 802.11a (теперь часть стандарта 802.11-2020) гласит что "OFDM PHY должен работать в полосе 5ГГц, выделенной регулирующим органом в своем рабочем регионе". Большинство стран разрешают OFDM передачи в каналах различных U-NII полос, которые обсуждаются в этой главе. Соединенные Штаты

**240** Глава 6 · Беспроводные Сети и Технологии Расширения Спектра  
также всегда разрешали OFDM передачи на канале 165, который, до Апреля 2014  
года, находился в полосе 5,8ГГц ISM. Исторически, канал 165 редко используется.  
В Апреле 2014 года, полоса U-NII-3 была расширена, чтобы включить канал 165.

С точки зрения каналов Wi-Fi полоса ISM 5,8 ГГц не имеет значения; однако, многие  
потребительские устройства, которые работают в полосе 5,8ГГц ISM могут вызвать  
радиоинтерференцию с радиосигналом 802.11, который передает в полосе U-NII-3.

## Нелицензируемые Полосы Национальной Информационной Инфраструктуры в 5ГГц

Поправка IEEE 802.11a определяла передачу БЛВС в частотном пространстве трех  
5ГГц полос, по четыре канала в каждой. Эти частотные диапазоны называются  
*Нелицензируемые Полосы Национальной Информационной Инфраструктуры*  
[*Unlicensed National Information Infrastructure (U-NII)*]. Поправка 802.11a определяла  
три группы, или полосы, частот U-NII, часто называемыми: нижняя, средняя и  
верхняя U-NII полосы. Эти три полосы обычно обозначаются как U-NII-1 (нижняя), U-  
NII-2 (средняя), and U-NII-3 (верхняя).

Когда была принята поправка 802.11h, IEEE определил больше частотного  
пространства для передачи БЛВС. Это частотное пространство, состоит из 12  
дополнительных каналов, изначально называлось как U-NII-2 Расширенные, а  
теперь называется полоса U-NII-2C.

Радиомодули Wi-Fi, которые на текущий момент передают в полосах 5ГГц U-  
NII, включают радиомодули, которые используют следующие технологии:

- 802.11a (радио OFDM)
- 802.11n (радио HT)
- 802.11ac (радио VHT)
- 802.11ax (радио HE)

Держите в уме, что не каждый государственный радиочастотный регуляторный орган  
разрешит передачу во всех этих трех полосах. Стандарт IEEE 802.11-2020 разрешает  
передачу БЛВС во всех четырех полосах U-NII по всем 25 каналам. Однако, в  
каждой стране может быть по-разному из-за различного регулирования каналов и  
мощности.

### U-NII-1

U-NII-1, нижняя полоса U-NII, имеет ширину 100 МГц и распространяется от  
5,150ГГц до 5,250ГГц. Суммарно четыре 20 МГц 802.11 канала находятся в полосе  
U-NII-1. В прошлом, полоса U-NII-1 была ограничена FCC только для использования  
внутри помещений в Соединенных Штатах. С Апреля 2014 года FCC опустила это  
ограничение. До 2004 года, FCC требовала, чтобы все устройства U-NII-1 имели  
несъемные антенны. Это значит, что любое устройство 802.11a, которое  
поддерживала U-NII-1, не могло иметь съемную antennу, даже если устройство  
поддерживало другие частоты или стандарты.

В 2004, FCC изменило правила, чтобы разрешить съемные антенны, при условии,  
что антенный разъем уникален. Это требование аналогично антенным требованиям

Нелицензируемые Полосы Национальной Информационной Инфраструктуры в 5 ГГц для других U-NII полос и полосы ISM 2,4ГГц. Всегда помните, что регуляторные правила на мощность и передачу в 5ГГц часто отличаются в других странах. Позаботьтесь о том, что вы не превышаете ограничения вашего локального регуляторного органа.

## **U-NII-2A**

Первоначальная полоса U-NII-2 теперь называется, как полоса U-NII-2A. U-NII-2A, изначально средняя полоса U-NII, в ширину 100МГц и располагается от 5,250ГГц до 5,350ГГц. Все четыре 20Мгц канала 802.11 находятся в полосе U-NII-2.

Радиомодули 802.11, которые передают в полосе U-NII-2A должны поддерживать динамический выбор частоты [*dynamic frequency selection (DFS)*].

## **U-NII-2C**

Полоса U-NII-2 Расширенная теперь более часто называемая как полоса U-NII-2C. Полоса U-NII-2C шириной 255 МГц и распространяется от 5,470ГГц до 5,725 ГГц. Большинство 5ГГц радиомодулей 802.11 могут передавать на всех одиннадцати 20Мгц каналах 802.11, которые располагаются в полосе U-NII-2. Однако, с появлением технологии 802.11ac был добавлен новый канал 144 к полосе U-NII-2C, всего 12 каналов. Нужно понимать, что много старых клиентских радиомодулей могут не поддерживать 144ый канал. Радиомодули 802.11, которые передают в полосе U-NII-2C должны поддерживать динамический выбор частоты (DFS). Работа БЛВС была в первые разрешена в этой полосе с принятием поправки 802.11h. До принятия этой поправки, БЛВС связь в 5 ГГц была разрешена только в U-NII-1, U-NII-2A, U-NII-3.

### **Динамический Выбор Частоты и Контроль Мощности Передачи**

В Главе 2, "Стандарты и Поправки IEEE 802.11", вы узнали, что поправка 802.11h определяет использование контроля мощности передачи (TPC) и динамического выбора частоты (DFS), чтобы избежать интерференции с передачей радара. Для любого продукта 5ГГц БЛВС, произведенного в Соединенных Штатах или Канаде с или после 20 июля 2007 года, требуется поддержка динамического выбора частоты, если он передает во всех полосах U-NII-2. Правила FCC требуют, чтобы продукты БЛВС, работающие в полосах U-NII-2, поддерживали DFS, чтобы защитить БЛВС связь от интерференции с военными или метеорологическими радарными системами. Европа также требует меры защиты DFS. DFS это механизм, который определяет присутствие сигналов радара и динамически заставляет передатчик переключаться на другой канал. До начала какой-бы то ни было передачи, радиостанция оснащенная DFS функционалом должна непрерывно мониторить радиосреду на предмет наличия передачи импульсов радара. Если радиостанция определяет, что сигнал радара присутствует, она должна или выбрать другой канал, чтобы избежать интерференции с радаром, или перейти в "спящий режим", если нет другого доступного канала. TPC требуется для защиты Спутниковой Службы Исследования Земли [Earth Exploration Satellite Service (EESS)]. И еще раз, локальные регуляторные органы определяют какие ограничения TPC и DFS применяются в каждой из полос U-NII. Более подробное обсуждение механизма DFS будет в Главе 13.

## U-NII-3

U-NII-3, верхняя полоса U-NII, шириной 125 МГц и распространяется от 5,725 ГГц до 5,850 ГГц. Эта полоса обычно используется для наружной связи точка-точка, но также может использоваться и внутри помещений в некоторых странах, включая Соединенные Штаты. В прошлом, многие страны в Европе не разрешали каналы в полосе U-NII-3 для связи без лицензии. Некоторые Европейские страны разрешали передачу в полосе U-NII-3 за приобретение недорогой лицензии. В последние годы, много стран в Европе открыли полосу U-NII-3 для Wi-Fi и другой нелицензионной радиосвязи.

В таблице 6.3, заметьте, что пять 20 МГц каналов 802.11 находятся в полосе U-NII-3. В апреле 2014 года FCC расширила размер полосы U-NII-3 со 100 МГц до 125 МГц. Канал 165, бывший в полосе 5,8 ГГц ISM, теперь доступен как часть полосы U-NII-3. Клиентские Wi-Fi радиомодули произведенные до 2014 года вероятно не поддерживают канал 165.

**ТАБЛИЦА 6.3** Полосы 5 ГГц U-NII

Полоса	Частота	Каналы
U-NII-1	5.15 ГГц–5.25 ГГц	4 канала
U-NII-2A	5.25 ГГц–5.35 ГГц	4 канала
U-NII-2C	5.47 ГГц–5.725 ГГц	12 каналов
U-NII-3	5.725 ГГц–5.85 ГГц	5 каналов

## U-NII-4

В январе 2013 года, FCC предложила две новых полосы U-NII для безлицензионного использования. Предполагалось, что первая предложенная полоса U-NII-2, будет занимать частотное пространство 5,35 ГГц - 5,47 ГГц и предоставило бы шесть 20 МГц каналов. Однако, FCC решила, что полоса U-NII-2B не будет сделана доступной для Wi-Fi. Хоть FCC отказывает в расширении Wi-Fi в полосу U-NII-2B, все еще существует возможность дополнительного частотного расширения на верху 5 ГГц полосы. Нужно отметить, что на момент перевода (2022) данная полоса уже отдана для использования Wi-Fi.

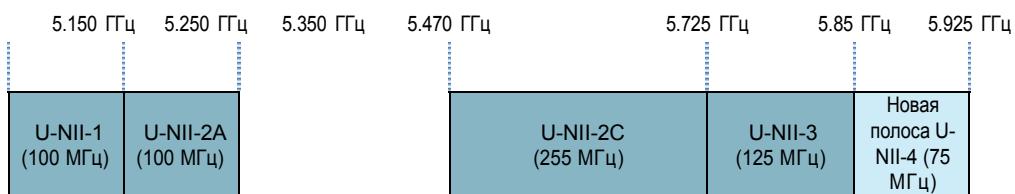
Регулирующими организациями США и Европы полоса частот U-NII-4, 5.85 ГГц – 5.925 ГГц, была зарезервирована декадой назад для *Беспроводного Доступа в Средах Транспортных Средств [Wireless Access in Vehicular Environments (WAVE)]* для связи транспортное средство – транспортное средство и транспортное средство – дорога. Это область 802.11p, и полоса обозначена как *выделенная связь на короткое расстояние [dedicated short-range communications (DSRC)]*.

Автомобильная промышленность ожидает значительные инновации в направлении самоуправляемых автомобилей и расширенных опций безопасности, таких как мониторинг слепых зон. Эти технологии часто называются как *интеллектуальная транспортная система [intelligent transportation system (ITS)]*.

На текущий момент, есть небольшое использование полосы U-NII-4 автомобильной промышленностью. Таким образом, есть размышления со стороны FCC о том, что эта полоса может быть поделена с традиционными пользователями Wi-Fi там, где DSRC не используется. В Ноябре 2019 года, FCC выпустил Уведомление о Предполагаемом Создании Правил [Notice of Proposed Rulemaking (NPRM)], чтобы переосмыслить правила для 75 МГц полосы U-NII-4. NPRM предлагает переназначить нижние 45 МГц полосы U-NII-4 для использования Wi-Fi и нелицензируемого использования. Верхние 30 МГц полосы U-NII-4 будут переутверждены для автомобильной ITS, использующей новую сотовую LTE технологию, называемую C-V2x. Сотовая связь транспортное средство-со-всем (Cellular vehicle-to-everything (C-V2X)) - это технология ITS, которая подразумевает способность транспортных средств связываться друг с другом и со всем что вокруг них(например: светофоры). NPRM также предлагает рассмотреть должны ли быть еще разрешены старые ITS технологии DSRC.

Хотя полоса U-NII-4 предлагает только 75 МГц частотного пространства, оно идеально располагается для соединения с полосой U-NII-3. Следовательно, как показано на Рисунке 6.13, U-NII-4 предлагает потенциально три дополнительных 20 МГц канала, два дополнительных 40 МГц канала, и один дополнительный 80 МГц канал. Также, FCC согласовала безлицензионную связь в большом количестве полос U-NII в частотном диапазоне 6ГГц. Полоса частот 6ГГц обсуждается позже в этой главе.

**РИСУНОК 6.13**      **U-NII-4**



## 60 ГГц для Wi-Fi

Как упоминалось в Главе 2, принятая поправка 802.11ad определяет использование направленных мульти-гигабитных (*directional multi-gigabit (DMG)*) радиомодулей, которые работают в нелицензируемой полосе частот 60ГГц. Новые улучшения уровней PHY и MAC имеют потенциал достичь скоростей вплоть до 7Гбит/с.

Поскольку эти ультравысокие частоты имеют трудности с проникновением через стены, технологию в основном предполагается использовать для обеспечения полосоемкой связью на короткие расстояния внутри помещений, такой как потоковое видео высокой четкости (HD). Первоначальная цель заключалась в том, чтобы точки доступа с трехдиапазонными радиомодулями обеспечивали доступ к Wi-Fi в полосах 2,4 ГГц, 5 ГГц и 60 ГГц. Для большей части, 60ГГц DMG радиомодули еще не нашли свой путь в точки доступа уровня предприятия.

Некоторые производители БЛВС предлагают уличные точки доступа 802.11ad для радиомостов точка-точка на небольшие расстояния между зданиями.

Широкое частотное пространство, доступное в 60ГГц, может предоставить стабильную скорость передачи данных в 2,5 Гбит/с в транзитном канале

связи, которые часто имеют высокие требования к полосе. Требуется очень прямая линия прямой видимости между двумя точками, передающими на 60 ГГц. Эти точки доступа обычно также имеют радиомодули на 5 ГГц в том же самом корпусе для отказоустойчивости. Из-за малой длины волны 60 ГГц сигнала, он чувствителен к интерференции, вызванной погодными условиями, такими как проливной дождь, поэтому обычно в эти точки доступа встраивается механизм автоматической отказоустойчивости, если канал связи 60 ГГц падает.

Хотя, по большей части, технология 802.11ad очень похожа на 802.11ac, пожалуйста, поймите, что технология 802.11ad обратно не совместима ни с какой другой технологией 802.11.

## Ниже 1 ГГц

IEEE также предложила использование других полос частот для Wi-Fi связи. Для большей части, эти полосы еще не используются. Эти полосы могут быть, а могут и не быть использованы в зависимости от изменений в правилах управляющих спектром регуляторных групп в различных странах. Более того, внедрение Wi-Fi в любое частотное пространство зависит от рыночных соображений производителей чипсетов Wi-Fi. Одним из примеров является использование частотного пространства ниже 1 ГГц.

Поправка 802.11ah определяла использование Wi-Fi на частотах ниже 1 ГГц. Нижние частоты означают низкую скорость передачи данных, но на более далекие расстояния. Предполагаемое использование 802.11ah - сети датчиков, транзитные каналы связи для сетей датчиков, и Wi-Fi, увеличенной дальности, например, умные дома, автомобили, забота о здоровье, промышленность, торговые сети и сельское хозяйство. Такая сеть устройств называется *Интернет Вещей* [*Internet of Things (IoT)*] или *Межмашинное взаимодействие* [*machine-to-machine (M2M)*].

Доступные частоты будут отличаться в разных странах. Например: 902-928 МГц нелицензируемые частоты ISM доступны в Соединенных Штатах, в то время как частоты 863-868 МГц вероятнее всего будут доступны в Европе, а частоты 755-787 МГц будут доступны в Китае. Стандарт 802.11-2020 называет 802.11ah как субигагерцевая [*Sub 1 GHz (SIG)*] радиосвязь.

## Каналы 2,4 ГГц

Чтобы лучше понять как используются устаревшие радиотехнологии 802.11 (DSSS), 802.11b (HR-DSSS) и 802.11g(ERP), важно знать как стандарт IEEE 802.11-2020 делит полосу 2,4 ГГц ISM на 14 отдельных каналов, указанных в Таблице 6.4. Хотя полоса 2,4 ГГц ISM разделена на 14 каналов, FCC или локальная регулирующая организация определяет какие каналы разрешено использовать. Таблица 6.4 также показывает пример того, как отличаются поддерживаемые каналы по странам.

**ТАБЛИЦА 6.4** 2.4 ГГц частотный канальный план

ID Канала	Центральная частота (ГГц)	США (FCC)	Канада (IC)	Большинство Европейских стран
1	2.412	X	X	X
2	2.417	X	X	X
3	2.422	X	X	X
4	2.427	X	X	X
5	2.432	X	X	X
6	2.437	X	X	X
7	2.442	X	X	X
8	2.447	X	X	X
9	2.452	X	X	X
10	2.457	X	X	X
11	2.462	X	X	X
12	2.467			X
13	2.472			X
14	2.484			

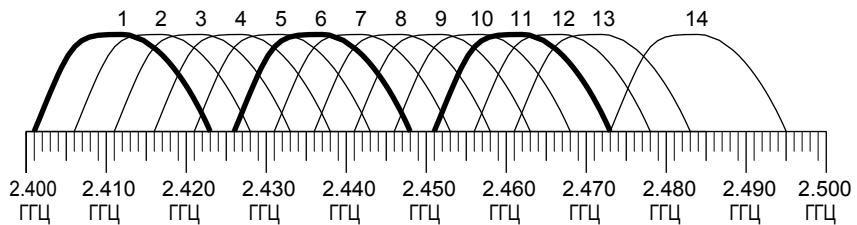
X = поддерживаемый канал

Каналы обозначаются своей центральной частотой. Насколько широк канал зависит от технологии, используемой передатчиком 802.11. Когда радиомодуль DSSS или HR-DSSS 802.11 передает, каждый канал имеет ширину 22 МГц, и часто обозначается как центральная частота  $\pm$  11 МГц. Например, канал 1 это 2,412 ГГц  $\pm$  11 МГц, что означает, что канал 1 расположен от 2,401 ГГц до 2,423 ГГц. Следует также отметить, что в полосе 2,4 ГГц ISM, расстояние между центральными частотами каналов всего лишь 5 МГц. Так как каждый канал имеет ширину 22 МГц, и так как расстояние между центральными частотами каждого канала только 5 МГц, каналы будут иметь перекрывающееся частотное пространство.

Все современные радиомодули используют OFDM и ширина полосы частот, используемая OFDM каналом, составляет примерно 20 МГц (как определено спектральной маской).

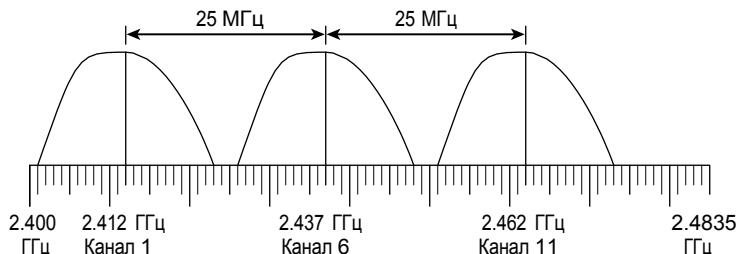
Рисунок 6.14 показывает наложение всех каналов и того, как они перекрываются. Каналы 1,6 и 11 выделены, потому что, как вы видите, они отделены друг от друга достаточным количеством частот так, что они не перекрываются. Для того, чтобы два канала не перекрывались, они должны быть отделены как минимум пятью каналами, или 25 МГц. Каналы, такие как 2 и 9 не перекрываются, но, когда выбраны 2 и 9, больше нет дополнительных легальных каналов, которые могут быть выбраны и не пересекаться со 2м или 9м. В Соединенных Штатах и Канаде, только три одновременно неперекрывающихся канала 1, 6 и 11. В регионах, где разрешены к использованию каналы с 1 по 13, существует другая комбинация трех неперекрывающихся канала, хотя обычно выбираются каналы 1,6 и 11. При развертывании на предприятии трех и более точек доступа в полосе 2,4ГГц ISM, используют каналы 1,6 и 11, которые считаются неперекрывающимися.

**Р И С У Н О К 6 .1 4** Диаграмма перекрытия 2,4ГГц каналов



Определения IEEE 802.11-2020 о неперекрывающихся каналах в полосе ISM 2,4ГГц может отчасти привести в замешательство, если правильно не объяснено. В полосе 2,4ГГц, каналы HR-DSSS и OFDM используют одну и ту же схему нумерации, и те же самые центры частот. Однако, индивидуальные частотные пространства каналов могут перекрываться. Рисунок 6.5 показывает каналы 1, 6 и 11 с 25МГц пространством между центрами частот. Это наиболее используемые неперекрывающиеся каналы в Северной Америке и большой части мира для сетей 802.11b/g/n/ax, развернутых в полосе 2,4 ГГц.

**Р И С У Н О К 6 .1 5** Центральные частоты в 2,4 ГГц



Как точно классифицировать каналы DSSS или HR-DSSS как неперекрывающиеся? В соответствии с оригинальным стандартом 802.11, старые каналы DSSS должны были иметь как минимум 30 МГц пространства между центральными частотами, чтобы считаться неперекрывающимися. При развертывании уже устаревшего оборудования DSSS, использующего канальный шаблон 1,6 и 11, каналы считались перекрывающимися, потому что центральные частоты были всего лишь 25МГц друг от друга. Хотя DSSS каналы 1,6 и 11 были определены как перекрывающиеся, только эти три канала по-прежнему использовались в модели переиспользования каналов при развертывании древних сетей. Это больше не имеет большого значения, так как большинство установок в 2,4ГГц теперь используют технологию 802.11b/g/n/ax.

HR-DSSS был представлен в поправке 802.11b, которая гласит, что каналам нужно минимум 25МГц между центральными частотами, чтобы считаться неперекрывающимися. Следовательно, когда был введен 802.11b, каналы 1, 6 и 11 считались неперекрывающимися.

Поправка 802.11g, которая допускает обратную совместимость с 802.11b HR-DSSS, также требует разделение в 15МГц между центральными частотами, чтобы считаться неперекрывающимися. В поправке 802.11g каналы 1,6 и 11 также считаются неперекрывающимися и для ERP-DSSS/CCK, и для ERP-OFDM. То же самое справедливо и при использовании каналов 802.11n OFDM и 802.11ax OFDMA в диапазоне 2,4 ГГц; фактически только каналы 1, 6 и 11 считаются неперекрывающимися.

Так почему мы используем столько места на страницах, чтобы обсудить перекрывающиеся и неперекрывающиеся каналы в полосе 2,4ГГц? В Главе 13 вы узнаете о моделях переиспользования 2,4ГГц каналов. И хотя существует 14 каналов в полосе 2,4ГГц, только 3 канала – 1, 6 и 11, могут быть эффективно использованы для развертывания БЛВС предприятия.



## Реальный Сценарий

### В чем значимость смежных каналов?

Большинство производителей Wi-Fi используют термин *интерференция смежных каналов* [*adjacent channel interference*] для названия ухудшения производительности в результате перекрывающегося частотного пространства, которое случается из-за неправильного плана переиспользования каналов. В области БЛВС, смежным каналом считается следующий или предыдущий по номеру канал. Например, канал 3 является смежным к каналу 2. Концепция интерференции смежных каналов подробно обсуждается в Главе 13.

## Каналы 5 ГГц

Радиомодули 802.11a/n/ac/ax передают в полосах 5ГГц U-NII: U-NII-1, U-NII-2A, U-NII-2C, в U-NII-3. Чтобы предотвратить интерференцию с другими возможными полосами, используется дополнительная полоса в качестве защитной полосы. В полосах U-NII-1 и U-NII-2, центры внешних каналов каждой полосы должны быть 30МГц от края полосы.

В полосе U-NII-3 существует дополнительные 20МГц полосы. Неиспользуемая полоса на краю каждой полосы называется *защитный интервал* или *защитная полоса [guard band]*. Каждые оригинальные три U-NII полосы имеют четыре неперекрывающиеся канала с расстоянием 20МГц между центральными частотами. Пятый канал был добавлен к U-NII-3. Полоса U-NII-2C имеет 12 неперекрывающихся каналов с расстоянием 20МГц между центральными частотами. Полоса U-NII-2C была 11 канальной полосой много лет, но дополнительный канал, 144, был добавлен к полосе с появлением 802.11ac. Если вы хотите высчитать центральную частоту канала, умножьте на 5 и затем добавьте 5000 к результату – например, канал 36 умноженное на 5 равно 180, затем добавляем 5000, для центральной частоты 5180 МГц, или 5,18ГГц.

Рисунок 6.16 показывает восемь U-NII-1 и U-NII-2A каналов наверху графика, 12 U-NII-2C каналов в центре графика, и пять U-NII-3 каналов внизу графика. Канал 36 выделен, чтобы было проще различать одну несущую и ее боковые частоты. IEEE специально не определял ширину канала, однако, спектральная маска OFDM канала примерно 20МГц.

**РИСУНОК 6.16** Каналы U-NII

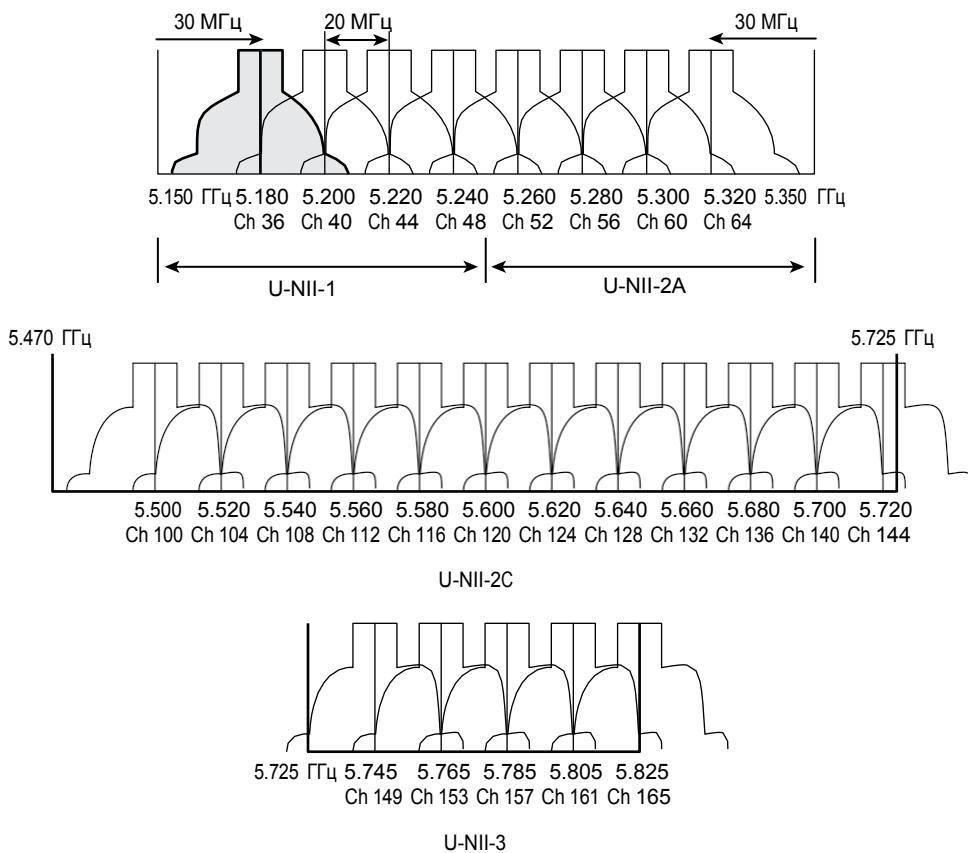
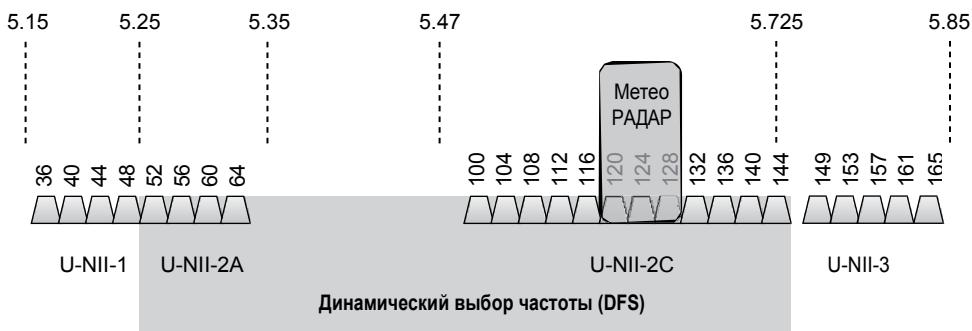


Рисунок 6.17 показывает широкий обзор всех 5 ГГц каналов, которые могут сегодня использоваться передатчиками 802.11. Всего двадцать пять 20МГц каналов в 5ГГц полосах U-NII могут быть использованы при проектировании БЛВС с моделью переиспользования каналов. Какие каналы вы можете использовать, конечно, зависит от регулирования каждой страны. Например, в некоторых странах, полоса U-NII-3 все еще считается лицензируемой полосой, что означает что только 20 каналов доступны для модели переиспользования каналов. В Соединенных Штатах, все каналы были доступны до 2009. Заметьте на Рисунке 6.17, что на каналах в U-NII-2A и U-NII-2C требуется DFS. В этих полосах требуется, чтобы радиомодули 802.11 использовали динамический выбор частоты (DFS) для предотвращения интерференции с радаром. В 2009 году Федеральное Управление Гражданской Авиации США [Federal Aviation Authority (FAA)] сообщило об интерференции с системами *Доплеровского Метеорологического Радара* [Terminal Doppler Weather Radar (TDWR)]. В результате, FCC вернула сертификацию устройств 802.11 в полосах U-NII-2 и U-NII-2E, которые требуют DFS. В итоге, сертификация была возобновлена; однако правила изменились и радиомодулям 802.11 не разрешалось передавать в пространстве частот 5,60 ГГц- 5,65 ГГц, где работает метеорадар TDWR. Как показано на рисунке 6.17, каналы 120, 124 и 128 располагаются в частотном пространстве TDWR и не могли использоваться долгие годы в Соединенных Штатах; следовательно, не все каналы были доступны для переиспользования 20МГц каналов. В 2014 году, FCC изменила правила и частотное пространство TDWR стало снова доступно. Следует также заметить, что некоторые установки БЛВС уровня предприятия полностью избегали использования каналов DFS, так как некоторые старые клиентские устройства никогда не поддерживали никакой DFS канал. Более подробное обсуждение модели переиспользования 5ГГц каналов и канального планирования появится в Главе 13.

**РИСУНОК 6.17** Обзор каналов U-NII



Технология 802.11n ввела функционал объединения вместе двух 20МГц каналов, чтобы создать больший 40 МГц канал. Объединение каналов (иногда вульгарно называемых бондингом) фактически удваивает ширину полосы частот, что означает удвоение скорости передачи данных, которые могут быть доступны радиомодулям 802.11n. 40 МГц каналы будут обсуждаться значительно детальнее в Главе 10. Как показано на рисунке 6.18, всего двенадцать 40 МГц каналов доступно к использованию в модели переиспользования при развертывании БЛВС предприятия. Однако, в прошлом, два из 40МГц каналов не использовались в Соединенных Штатах, потому что они попадали в полосу метеорадара TDWR. В Европе, два 40МГц исторически были не доступны, потому что они попадали в полосу U-NII-3, которая требует лицензирования.

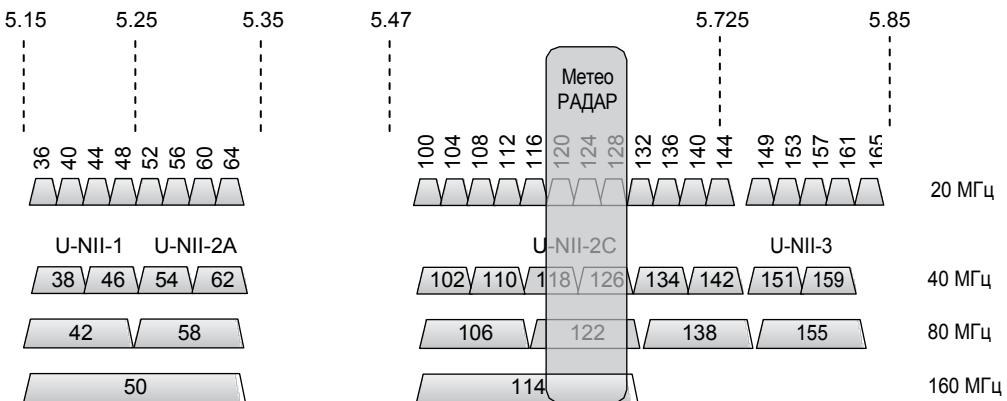
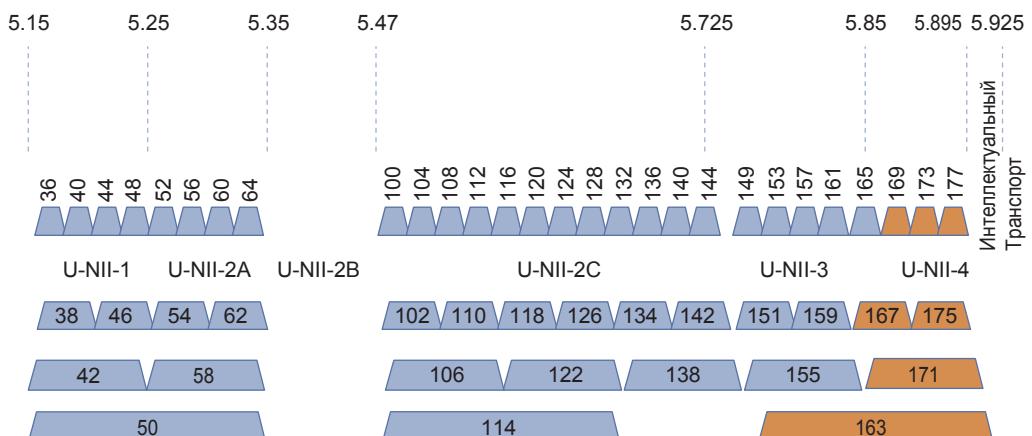


Рисунок 6.18 также показывает 80МГц каналы и 160МГц каналы, которые могут быть потенциально использованы радиомодулями 802.11ac/ax. В действительности, нет достаточного частотного пространства, чтобы обеспечить достаточное количество этих каналов для соответствующих моделей переиспользования каналов. Возможности 802.11ac/ax, включающие 80МГц и 160МГц каналы, обсуждаются в Главе 10.

По мере того как технология 802.11ac/ax становится более общепринятой, необходимость в дополнительном (экстра) частотном пространстве стала даже более важной. Как показано на Рисунке 6.19, если спектр U-NII-4 действительно сделают доступным, модель переиспользования широких каналов станет возможной. Всего четырнадцать 40МГц каналов тогда было бы доступно для радиомодулей 802.11n/ac и 802.11ac/ax. А модель переиспользования семи 80 МГц каналов тогда может быть спланирована для использования радиомодулями 802.11ac/ax. Тогда было бы даже достаточно частотного пространства для трех 160 МГц каналов в полосе 5ГГц. Пожалуйста, держите в уме, что предложенный дополнительный спектр (экстрапектр) все-еще на текущий момент не доступен и, что правила и регулирование использования частот могут варьироваться от страны к стране. Наоборот, использование экстрашироких каналов на предприятиях будет более вероятно становиться общей практикой с доступностью 6ГГц частотной полосы.

**РИСУНОК 6.19** Потенциальные 40 МГц, 80 МГц, и 160 МГц каналы



## Долгосрочная Эволюция (Long-Term Evolution(LTE)) в 5 ГГц

И хотя эта книга о беспроводной технологии 802.11, существуют другие радиоволновые технологии, с которыми вам следует быть знакомыми, включая Bluetooth, Zigbee, и сотовую технологию. *Долгосрочная Эволюция [Long-Term Evolution (LTE)]* - это стандарт для высокоскоростной беспроводной связи для голоса и передачи данных для сотовых устройств. Следующее поколение технологии LTE, на текущий момент создающее много статей – это Беспроводные Системы Пятого Поколения [Fifth-Generation Wireless Systems], также называемые как 5G (пять джи). В отличие от предыдущих поколений технологии LTE, 5G использует и нелицензируемый, и лицензируемый спектр для сотовой связи.

Вы можете услышать термины 5G и нелицензируемый LTE, которые используются взаимозаменямо. Это не верно. Страйтесь думать о 5G как о структуре, вмещающей и технологию, и коммерческое использование, где нелицензируемый LTE – это одна из множества сотовых технологий, потенциально используемая, в среде 5G. В рамках этой главы, взаимосвязь между нелицензируемым LTE и Wi-Fi является главным обсуждением.

Одна из главных причин, почему БЛВС предприятий разворачиваются в нелицензируемой полосе 5ГГц, это то, что нелицензируемая полоса 2,4ГГц уже переполнена. Более того, 5ГГц имеет больше частотного пространства и традиционно в основном используется для Wi-Fi связи. Однако, сотовые компании успешно лоббируют LTE связь в нелицензируемой 5ГГц полосе частот, где сейчас работает Wi-Fi.

Будут ли нелицензируемые LTE передачи в 5ГГц полосе частот интерферировать с Wi-Fi (и наоборот)? Ответ – да, но на сколько сильно зависит от нескольких переменных. Сначала вам следует осознать, что много разновидностей LTE определено для использования в нелицензируемом спектре, включая полосу 5ГГц.

Интеграторы и проектировщики Wi-Fi должны знать возможности нелицензируемого LTE. Запомните, что это очень упрощённый обзор; и когда столкнетесь с задачей проектирования в присутствии нелицензируемого LTE, просто делайте свою работу. Некоторые технологии нелицензируемого LTE включают следующее:

**LTE-U** Технология Нелицензируемого LTE [LTE-Unlicensed (LTE-U)] используется в нелицензируемых полосах U-NII-1 и U-NII-3 в 5ГГц спектре. LTE-U использует 20МГц каналы для нисходящей [downlink] связи от базовой станции LTE-U. Восходящая [uplink] связь и управление [control plane] остаются в лицензируемом спектре. Телеком операторы агрегируют нелицензируемые 5ГГц нисходящие [downlink] каналы связи вместе с восходящими [uplink] каналами связи, работающими в лицензируемом (400МГц – 3,8ГГц) якорном канале. LTE-U не применяет никакой механизм защиты «слушай прежде, чем говорить» (“listen before talk”) и передает по Wi-Fi связи в том же частотном пространстве. LTE-U использует алгоритм Адаптивной Передачи с Контролем Несущей [Carrier Sense Adaptive Transmission (CSAT)]. CSAT динамически выбирает свободный канал, чтобы избежать интерференции с Wi-Fi. Однако, если нет ни одного свободного канала, CSAT совместно использует канал, используя состояния вкл/выкл рабочего цикла сигнала, который обеспечивает 50 процентов рабочего цикла для LTE и 50 процентов рабочего цикла для Wi-Fi связи на 5ГГц канале.

**LTE-LAA** Другая технология LTE предназначенная для нелицензируемых частот – это Лицензионный Вспомогательный Доступ [License Assisted

**252** Глава 6 • Беспроводные Сети и Технологии Расширения Спектра Access (*LAA*]), который изначально был определен только для нисходящей [downlink] связи. Новый вариант, названный улучшенный Лицензионный Вспомогательный Доступ [*enhanced Licensed Assisted Access (eLAA)*] поддерживает и восходящую связь[uplink]. eLAA использует каналы до 20МГц ширины, но может работать двунаправленно для передачи данных. eLAA использует и лицензируемый и нелицензируемый спектр для данных, но использует лицензируемый спектр для управления. LTE-LAA также использует операторскую агрегацию нелицензируемого 5ГГц канала вместе с лицензируемым якорным каналом.

LTE-LAA использует “Слушай Прежде, Чем Говорить” [*Listen Before Talk (LBT)*] в качестве защитного механизма по обнаружению несущей, отчасти похожего по характеристикам на оценку чистоты канала [*clear channel assessment (CCA)*], используемой радиомодулями 802.11. Базовая станция LTE-LAA использует порог обнаружения радиоволновой энергии [*energy detect (ED)*], чтобы задержать передачу LTE. Однако нет порога обнаружения сигнала [*signal detect (SD)*] для конкретного обнаружения передачи 802.11. Во время написания книги, LTE-LAA избегает передачи на DFS каналах.

**MulteFire (произносится МултиФайя)** На текущий момент, *MulteFire* работает исключительно в нелицензируемой 5ГГц полосе для нисходящей связи, восходящей связи и связи для управления. Не требуется лицензируемый якорный канал, и, следовательно, нет операторского агрегирования. *MulteFire* предназначен для развертывания небольших сот, и для всех предполагаемых целей, *MulteFire* можно рассматривать как прямого конкурента Wi-Fi. Аналогично LTE-LAA, *MulteFire* использует “Слушай Прежде, Чем Говорить” [*Listen Before Talk (LBT)*] в качестве защитного механизма по обнаружению несущей. *MulteFire* также работает на 20МГц каналах.

**LTE-WLAN Aggregation** *LTE-БЛВС Агрегация* [*LTE-WLAN Aggregation (LWA)*] предоставляет альтернативу LTE в 5 ГГц спектре. Передача данных LTE остается в лицензируемом канале, в то время как Wi-Fi связь остается в нелицензируемом канале. Однако, LWA обеспечивает агрегацию данных через оба канала связи, как одного потока трафика данных. Мобильные устройства, которые поддерживают и LTE и Wi-Fi могут быть сконфигурированы, чтобы использовать оба канала связи одновременно. С точки зрения Wi-Fi, основное преимущество в том, что не нужно совместно использовать 5ГГц канал, потому что LTE связь остается в лицензируемом спектре.

Из-за политического влияния и лоббирования сотовыми операторами и производителями микросхем (чипсетов), нелицензируемый LTE в полосе 5ГГц медленно становится реальностью в некоторых регионах. Остается только наблюдать, какая нелицензируемая технология LTE станет наиболее превалирующей, а различные регионы мира смогут принять различные стандарты нелицензируемого LTE. Помните, что LTE должен будет следовать тем же самим правилам по мощности передачи в нелицензируемой полосе 5ГГц, что и Wi-Fi. Однако, большинство установок точек доступа WI-Fi внутри помещений используют максимум 100мВт, в то время как базовая станция LTE может передавать с мощностью 1 ватт. Несмотря на определенные методы сосуществования, можно с уверенностью предположить, что между LTE и Wi-Fi будет возникать интерференция. По мере того, как нелицензируемый LTE продвигается в полосу 5 ГГц, могут стать неизбежными новые проблемы для проектирования и развертывания БЛВС. В последние годы, частный LTE для передачи данных стартовал в Соединенных Штатах. Частный[*Private*] LTE работает в лицензируемых частотах, которые не влияют на полосу

5ГГц или другие нелицензируемые частоты, используемый для Wi-Fi.

## Каналы 6 ГГц

Wi-Fi Альянс начал сертифицировать технологию 802.11ax в Августе 2019 года, в новой сертификации, названной СЕРТИФИЦИРОВАННЫЙ WI-FI 6 [Wi-Fi CERTIFIED 6]. Наиболее актуальной технологией для Wi-Fi 6 является OFDMA. Wi-Fi Альянс требует обязательную поддержку OFDMA для исходящего канала [downlink] и для восходящего канала [uplink] как в полосе частот 2.4ГГц, так и 5ГГц. Детальную информацию о 802.11ax можно найти в Главе 19.

В начале 2020, FCC проголосовало неанонимно сделать 1200 мегагерц спектра в 6ГГц полосе доступными для нелицензируемого использования в Соединенных Штатах. Первая точка доступа Wi-Fi 6 уровня предприятия будет доступна к работе в этой полосе в начале 2021 года. Чтобы представить это в перспективе, новый спектр 6 ГГц, доступный для Wi-Fi, содержит более чем вдвое большее количество используемых каналов 2,4 ГГц и 5 ГГц вместе взятых.

В предсказании доступности этого частотного пространства, Wi-Fi Альянс анонсировал сертификацию Wi-Fi 6E в качестве «расширения» для сертификации тех же самых характеристик и возможностей 802.11ax Wi-Fi 6 в полосе 6 ГГц.

Ключевая разница использования 6ГГц полосы частот для технологии 802.11ax это то, что не нужна обратная совместимость. Так как радиомодули 802.11a/b/g/n/ac работают только в полосах 2,4ГГц и 5ГГц, и не работает в 6ГГц полосе, то не нужен механизм защиты. Полоса частот 6ГГц будет «чистой» полосой технологии 802.11ax для Wi-Fi связи. Полоса 6ГГц является также более чистым спектром без требования поддержки динамического выбора частоты, необходимой для избегания радара. В диапазоне 6 ГГц есть некоторые действующие передатчики, для которых требуется другой тип защиты от интерференции, который будет обсуждаться далее в этом разделе.

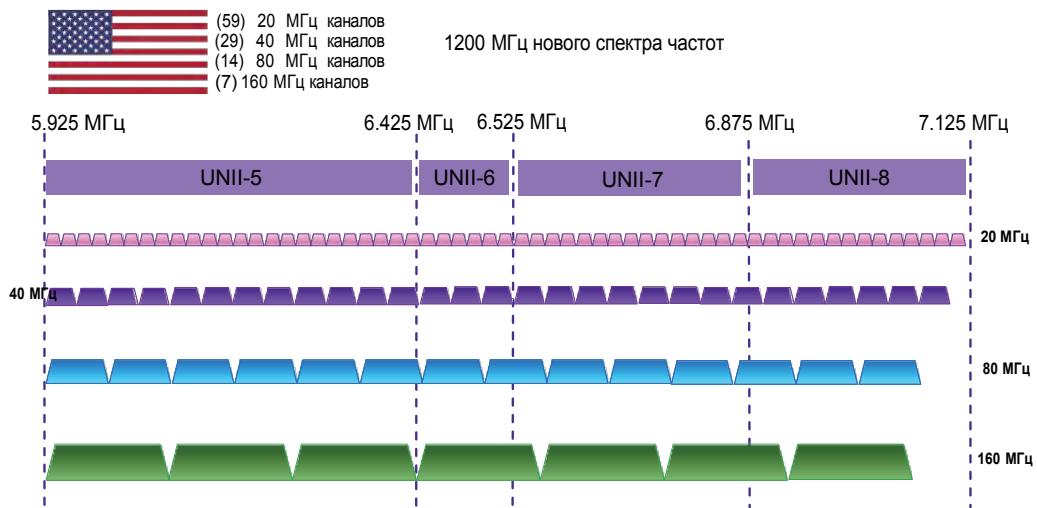
Производители БЛВС будут создавать точки доступа Wi-Fi 6E во множестве различных корпусах, но в большинстве случаев они будут содержать радиомодули всех трех полос (2,4, 5 и 6 ГГц). Однако, только новые клиентские устройства Wi-Fi 6E с радиомодулями 6ГГц будут способны поддерживать связь с 6ГГц радиомодулем в точке доступа Wi-Fi 6E. Старый двухдиапазонный (2,4 и 5 ГГц) смартфон будет способен установить связь только с радиомодулями 2,4 и 5 ГГц в трехдиапазонной Wi-Fi 6E точке доступа. Таблица 6.5 показывает краткое сравнение различных поколений Wi-Fi.

**ТАБЛИЦА 6.5** Сравнение поколений Wi-Fi технологий

Технология	Wi-Fi 4 (802.11n)	Wi-Fi 5 (802.11ac)	Wi-Fi 6 (802.11ax)	Wi-Fi 6E (802.11ax в 6 ГГц)
Полосы частот	2.4 & 5 ГГц	5 ГГц	2.4 & 5 ГГц	6 ГГц
Максимально доступное количество 20МГц каналов для переиспользования	3 канала в 2.4 ГГц	N/A	3 канала в 2.4 ГГц	59 каналов в 6 ГГц
	25 каналов в 5 ГГц	25 каналов в 5 ГГц	25 каналов в 5 ГГц	
Доступная полоса	60 МГц в 2.4 ГГц	N/A	60 МГц в 2.4 ГГц	1200 МГц в 6 ГГц
	500 МГц в 5 ГГц	500 МГц в 5 ГГц	500 МГц в 5 ГГц	
Размер канала (МГц)	20 & 40	20, 40, 80, 80 + 80, 160	20, 40, 80, 80 + 80, 160	20, 40, 80, 80 + 80, 160
Частотное мультиплексирование	OFDM	OFDM	OFDM & OFDMA	OFDM & OFDMA
Многопользовательская технология	N/A	MU-MIMO (DL)	MU-MIMO (DL & UL)	MU-MIMO (DL & UL)
			OFDMA (DL & UL)	OFDMA (DL & UL)
Wi-Fi безопасность	Open	Open	Open	Enhanced Open (обязательно)
	WPA2	WPA2	WPA2	N/A
	WPA3 (оpционально)	WPA3 (оpционально)	WPA3	WPA3 (обязательно)
Обратная совместимость	Есть	Есть	Есть	Нет*

\* Точка доступа и клиенты будут обратно совместимы в том смысле, что они могут поддерживать несколько полос, однако, только радиомодули Wi-Fi 6E могут передавать в каналах 6ГГц.

Потенциал 1200МГц нового частотного пространства для Wi-Fi ошеломляет. Ожидается, что открытие частоты 6 ГГц для Wi-Fi принесет Соединенным Штатам экономическую выгоду в размере 154 миллиардов долларов к 2025 году. Как показано на Рисунке 6.20, в Соединенных Штатах будет 59 новых 20 МГц каналов, доступных во всех четырех U-NII полосах.

**РИСУНОК 6.20** 6 ГГц U-NII полосы и каналы Wi-Fi (Соединенные Штаты)


Будут установлены мощностные регуляторные правила о том, как полосы могут быть использованы. FCC разрешает использование всей полосы 6ГГц и всех четырех U-NII полос для использования внутри помещений. Как показано в Таблице 6.6, новому классу устройств *маломощных точек доступа [low-power APs]* будет разрешено передавать внутри помещений только с максимальной ЭИИМ в 30дБм. Дополнительно, клиенты могут подключаться к маломощным внутренним точкам доступа с максимальной ЭИИМ 24дБм. FCC также будет требовать, чтобы все маломощные устройства включали в себя постоянно прикрепленные встроенные антенны. Требование встроенной антенны делает значительно более сложным замену антенны устройства на antennу с большим усилением FCC определил, что, следуя этим мощностным ограничениям внутри помещений, не будет создавать помехи уже существующим сервисам вне помещений. В результате, фактически вся полоса 6ГГц будет доступна для Wi-Fi внутри помещений.

**ТАБЛИЦА 6.6** Расширенное безлицензионное использование полосы 6ГГц (Соединенные Штаты)

Класс устройства	Рабочая полоса	Максимальные ЭИИМ(FIRP)
Маломощная точка доступа (только для использования внутри помещений)	U-NII-5 (5.925–6.425 ГГц) U-NII-6 (6.425–6.525 ГГц) U-NII-7 (6.525–6.875 ГГц) U-NII-8 (6.875–7.125 ГГц)	30 дБм
Клиент, подключенный к маломощной точке доступа	U-NII-5 (5.925–6.425 ГГц) U-NII-7 (6.525–6.875 ГГц)	24 дБм
Точка доступа стандартной мощности (AFC controlled)	U-NII-5 (5.925–6.425 ГГц) U-NII-7 (6.525–6.875 ГГц)	36 дБм
Клиент, подключенный к точке доступа стандартной мощности		30 дБм

## Существующие пользователи 6 ГГц

В Соединенных Штатах, правила для внешнего Wi-Fi в 6 ГГц полосе будут совершенно другими от того, что разрешено внутри помещений. Как показано в Таблице 6.7, уже существующие сервисы уже передающие во всех полосах U-NII 6ГГц. Полосы U-NII-6 и U-NII-8 будут не доступны для всей нелицензируемой внешней связи. U-NII-6 и U-NII-8 уже лицензируется и для мобильных спутниковых сервисов, и для фиксированных спутниковых сервисов [*fixed satellite services (FSS)*], используемых в отраслях телевидения и в отрасли кабельного вещания.

Следовательно, эти две полосы будут недоступны для любого внешнего Wi-Fi. FCC определяет еще один класс устройств *точка доступа стандартной мощности [standard-power AP]* для нелицензируемой связи вне помещений в полосах U-NII-5 и U-NII-7.

Максимальная ЭИИМ(EIRP) для точки доступа стандартной мощности будет 36дБм. Клиенты, которые подключаются к точке доступа стандартной мощности, могут иметь максимальную ЭИИМ 30дБм. Дополнительно, будут введены ограничения управления спектром, чтобы защитить лицензируемые существующие фиксированные сервисы в полосах U-NII-5 и U-NII-7. Эти ограничения нужны, чтобы защитить микроволновые сервисы точка-точка [point-to-point (PtP)].

**ТАБЛИЦА 6.7** Существующие сервисы в 6ГГц и наружный Wi-Fi

Полоса U-NII	Сервис	Существующий сервис	Wi-Fi вне помещений
U-NII-5	Фиксированная связь, FCC	Фиксированная микроволновая связь, FCC (каналы земля-спутник)	Да, требуется AFC
U-NII-6	Мобильная связь, FCC	Теле радио вещание [broadcast], ретрансляция кабельного ТВ, FCC (каналы земля-спутник)	Нет
U-NII-7	Фиксированная связь, FCC	Фиксированная микроволновая связь, FCC (каналы земля-спутник/спутник-земля)	Да, требуется AFC
U-NII-8	Фиксированная связь, Мобильная связь, FCC	Телерадиовещание [broadcast], фиксированная микроволновая связь, ретрансляция кабельного ТВ, FCC (каналы земля-спутник/спутник-земля)	Нет

## Автоматизированная Координация Частот

Для Wi-Fi связи вне помещений в полосах U-NII-5 и U-NII-7 FCC сделает обязательным использование *автоматизированной координации частот [automated frequency coordination (AFC)]*, чтобы защитить уже существующие сервисы в этих полосах. Система AFC будет использовать базы данных геолокации, чтобы управлять назначением частот в

реальном времени, чтобы защитить работу существующих устройств от радиоинтерференции. Перед тем как передавать, точке доступа стандартной мощности потребуется получить от AFC системы список разрешенных частот или список запрещенных частот, на которых нельзя передавать. Географические координаты точки доступа должны автоматически определяться по GPS или аналогичным надежным способом до проверки в системе AFC.

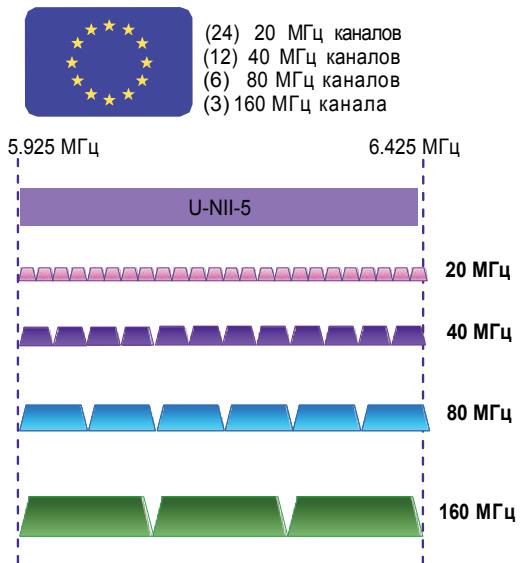
Например, вы можете захотеть развернуть внешнюю точку доступа стандартной мощности в Брукхейвен, штат Джорджия. Используя или GPS, или другой метод, определяется, что широта точки доступа 33.865105, а долгота 84.336594. Затем, точка доступа использует автоматическую систему для регистрации своих координат в одобренном FCC провайдере системы AFC. Высота точки доступа также принимается во внимание. База данных провайдера системы AFC автоматически проверяет на возможную интерференцию с уже существующими устройствами этого диапазона. Система AFC будет использоваться для определения запретных зон, где работа точек доступа стандартной мощности может пагубно воздействовать на уже существующие каналы связи в полосах U-NII-5 и U-NII-7. Если уже существующий в этом диапазоне микроволновой сервис существует поблизости, то на точку доступа Wi-Fi стандартной мощности принудительно применяется трехмерная защита AFC. Простыми словами, точке доступа может быть не разрешено передавать, или может быть приказано уменьшить мощность передачи значительно ниже 36дБм, чтобы избежать интерференции с уже существующими сервисами. Если поблизости нет уже существующих сервисов в этом диапазоне, то точка доступа может передавать.

Хотя FCC успешно использует координированные системы управления спектром на других полосах частот, все правила AFC и провайдеры систем еще не готовы. Следовательно, маломощные 6ГГц точки доступа только для использования внутри помещений выйдут на рынок раньше чем внешние точки доступа стандартной мощности станут доступными на коммерческом рынке.

Существует также некоторая дискуссия на тему разрешения использования мобильных точек доступа очень малой мощности в 6 ГГц. Другим словами, разрешение на использование 6ГГц Wi-Fi в автомобилях, поездах, и других транспортных средствах. Однако, на текущий момент, FCC запрещает работу 6ГГц Wi-Fi на транспорте из-за возможности увеличения интерференции с уже существующими сервисами. Есть одно заметное исключение в полосе U-NII-5 в отношении больших пассажирских самолетов, летающих выше 10000 футов (3048 метра). Маломощные точки доступа можно использовать в бортовых системах развлечения на больших пассажирских самолетах на высоте выше 10000 футов (3048 метров).

## 6 ГГц в Мире

Следует отметить, что все эти правила FCC в 6ГГц являются предметом изменений. Как вы узнали в главах ранее, все международные регулирующие организации по управлению спектром работают совместно друг с другом. Следовательно, другие регионы мира также ожидают открытия частотного пространства 6ГГц для нелицензируемого Wi-Fi. Как показано на Рисунке 6.21, ожидается, что 500МГц частотного пространства 6ГГц будет сделано доступным в большей части Европы где-то в 2021 году. Европейские регуляторы сосредоточились только на полосе U-NII-5 (5,925 - 6,425ГГц). Другие регионы мира также следуют за этим, но каждый будет иметь собственные правила и ограничения для нелицензируемого использования Wi-Fi в полосе частот 6ГГц.



В Соединенных Штатах будет доступно всего пятьдесят девять 20МГц каналов, а в Европе будет доступно двадцать четыре 20МГц каналов. Если выбрано 40МГц каналы, то 29 может быть использовано в США и 12 в Европе. На предприятиях, каналы 80МГц и 160МГц используются редко в 5ГГц полосе. Однако, полоса 6ГГц предлагает более 14 80 МГц каналов и более 7 160МГц каналов. Все эти каналы будут определены центральной частотой и иметь номер для идентификации. Например, Рисунок 6.22 показывает назначение каналов для 20МГц, 40МГц, 80МГц и 160МГц каналов в полосе U-NII-5.

**Р И С У Н О К 6 . 2 2** Каналы полосы U-NII-5

		UNII-5																										
		5.955	5.975	5.995	6.015	6.035	6.055	6.075	6.095	6.115	6.135	6.155	6.175	6.195	6.215	6.235	6.255	6.275	6.295	6.315	6.335	6.355	6.375	6.395	6.415			
20 МГц	1	5	9	13	17	21	25	29	33	37	41	45	49	53	57	61	65	69	73	77	81	85	89	93				
40 МГц	3		11		19		27		35		43		51		59		67		75		83		91					
80 МГц		7			23				39				55				71				87							
160 МГц			15						47								79											

## Рассуждения о 6 GHz Wi-Fi

Доступность частотного пространства 6ГГц для Wi-Fi будет иметь все виды последствий реального мира. ASUS анонсировала первый домашний Wi-Fi 6E маршрутизатор, доступный к покупке в рознице в Северной Америке в Декабре 2020года. Как ранее утверждалось, все основные производители БЛВС для предприятий ждут, чтобы предложить трех полосные точки доступа Wi-Fi 6E где-то в 2021 году. Однако, за доступностью клиентов Wi-Fi 6E с функционалом 6ГГц остается только наблюдать. В результате, один из быстрых вариантов использования, ожидаемых для Wi-Fi 6ГГц, это транзитный канал для взаимосвязанных [mesh] точек доступа внутри помещений. Устаревшие клиенты 2,4ГГц и 5 ГГц будут подключаться к точке доступа, а 6ГГц радиомодуль точки доступа может использоваться для организации mesh канала связи. Так как

системы AFC доступны для 6ГГц точек доступа стандартной мощности, уличные высокоскоростные взаимосвязные [mesh] каналы связи также будут реальностью.

Пройдет минимум несколько лет чтобы 6ГГц клиентские устройства стали большинством на предприятиях. По мере роста количества клиентских устройств 6ГГц, использование высокоскоростных приложений может стать обычным явлением. Например, приложения дополненной реальности [augmented reality (AR)] и виртуальной реальности [virtual reality (VR)] может потребовать где угодно от 10Мб/с до 100Мб/с полосы на клиента. AR/VR и компьютерные игры [gaming] являются великим вариантом использования для 6ГГц полосы. Много существующих высоко качественных шлемов/очков виртуальной реальности, которые требуют большую полосу, подключены кабелями. Ширина полосы частот, доступная в 6ГГц, может предоставить новые возможности для беспроводных приложений AR/VR.

По мере роста 6ГГц клиентских устройств, БЛВС должны проектироваться, чтобы обеспечить покрытие в 6ГГц. В Главе 13, вы узнаете о планах переиспользования каналов 20МГц и 40МГц в 5ГГц полосе частот. БЛВС, развернутые в сценариях высокой плотности, таких как спортивные залы, конференц-залы, стадионы, и другие места массового скопления обычно используют только планы переиспользования 20МГц каналов. Из-за доступности всего частотного пространства 6ГГц, ожидается, что использование планов переиспользования 40МГц каналов станет намного более распространенным. Планы 80МГц каналов могут также стать реальностью в 6ГГц полосе частот.

Как уже ранее упоминалось, потребуется время, чтобы клиентские устройства 6ГГц заполнили рынок и нашли свой путь для применения на предприятиях. Имейте в виду, что большинство устаревших клиентов никуда не денутся. Однако, когда клиентские устройства Wi-Fi 6E войдут на рынок, будут улучшенные механизмы обнаружения точек доступа, которые будут обсуждаться в Главе 13. Если точка доступа, работающая на 6ГГц канале, также имеет радиомодули, работающие в 2,4 и 5 ГГц каналах с тем же самым SSID, то радиомодули передающие в 2,4 и 5 ГГц будут сообщать информацию о 6ГГц канале в кадрах-маяках [beacon] и зондирующих ответных кадрах [probe response] клиенту с поддержкой Wi-Fi 6E. Это значительно уменьшит время клиентского зондирования и потенциально позволит клиентскому устройству ассоциироваться с 6ГГц радиомодулем точки доступа без необходимости сканирования всех трех диапазонов.

## Итого

Эта глава фокусировалась на различных технологиях расширения спектра, используемых в радиомодулях Wi-Fi. Большинство из радиомодулей первоначального 802.11, произведенных между 1997 и 1999, использовали скачкообразную перестройку частоты. Радиомодули 802.11b используют HR-DSSS, в то время как радиомодули 802.11a/g представили OFDM. Каждая технология расширения спектра определяет и модуляцию, и способы кодирования. Мы также обсудили спектральные маски передачи для HR-DSSS и для OFDM. Радиомодули 802.11n/ac продолжили использование OFDM, а 802.11ax принес нам многопользовательскую технологию OFDMA.

Эта глава также покрывает следующие полосы частот и каналов, в которых могут работать радиомодули 802.11:

- <1 ГГц
- 2.4 ГГц

- 5 ГГц
- 6 ГГц
- 60 ГГц

## Темы Экзамена

**Знать технические характеристики всех полос ISM и U-NII.** Убедитесь, что вы знаете все частоты, используемые ширины полос, и каналы.

**Знать расширение спектра.** Расширение спектра может быть сложным и иметь различные реализации. Понимать FHSS, DSSS, и OFDM. (Хотя OFDM не является технологией расширения спектра, она имеет похожие свойства, и вы должны знать об этом.) Понимать, как работает кодирование и модуляция с расширением спектра и OFDM.

**Понимать схожести и различия между методами передачи, обсужденных в этой главе.**

Существуют различия и схожести во многих темах в этой главе. Внимательно сравните и поймите их. Неосновные тонкости может быть трудно различить при прохождении экзамена.

# Контрольные вопросы

1. Какая технология имеет большую устойчивость к разбросу задержки?
  - A. DSSS
  - B. FHSS
  - C. OFDM
  - D. HR-DSSS
2. Что часто используется чтобы описать "форму" частотного канала? (Выберите все, что применимо.)
  - A. Максимальная спектральная плотность
  - B. Спектральная маска передачи
  - C. Радиоспектр
  - D. Спектральная маска
3. Какой термин лучше всего описывает точность модуляции?
  - A. EVM
  - B. ERP
  - C. VHT
  - D. QAM
4. 802.11n (НТ радиомодули) могут передавать в каких полосах частот? (Выберите все, что применимо.)
  - A. 2.4 ГГц–2.4835 ГГц
  - B. 5.47 ГГц–5.725 ГГц
  - C. 902 ГГц–928 ГГц
  - D. 5.15 ГГц–5.25 ГГц
5. Сколько 312,5 кГц поднесущих использует 20 МГц OFDM канал, чтобы модулировать данные, при передаче с помощью радиомодуля 802.11a/g?
  - A. 64
  - B. 52
  - C. 48
  - D. 36
6. Какие из этих клиентских радиомодулей будут способны передавать в полосе U-NII-5?
  - A. Клиентские радиомодули Wi-Fi 4
  - B. Клиентские радиомодули Wi-Fi 5
  - C. Клиентские радиомодули Wi-Fi 6
  - D. Клиентские радиомодули Wi-Fi 6E
  - E. Клиентские радиомодули Wi-Fi 7

7. Какая ширина полосы частот стандартного OFDM канала?
  - A. 20 МГц
  - B. 22 МГц
  - C. 25 МГц
  - D. 40 МГц
  - E. 80 МГц
  - F. 160 МГц
8. Что лучше всего описывает время перестроения (скакка) ?
  - A. Период времени, который ждет передатчик прежде чем перестроиться на следующую частоту.
  - B. Период времени, который требует стандарт при перестроении между частотами
  - C. Период времени, который нужен передатчику, чтобы перестроиться на следующую частоту
  - D. Период времени, который нужен передатчику, чтобы перестроится через все частоты FHSS
9. В соответствии со стандартом IEEE 802.11-2020, какое расстояние необходимо между центральными частотами в полосе U-NII-2C?
  - A. 10 МГц
  - B. 20 МГц
  - C. 22 МГц
  - D. 25 МГц
  - E. 30 МГц
10. Какая из этих технологий 802.11 может работать в полосе частот 5ГГц? (Выберите все, что применимо)
  - A. 802.11a (радиомодули OFDM)
  - B. 802.11b (радиомодули HR-DSSS)
  - C. 802.11g (радиомодули ERP)
  - D. 802.11n (радиомодули HT)
  - E. 802.11ac (радиомодули VHT)
  - F. 802.11ax (радиомодули HE)
11. Какая полоса U-NII на текущий момент предназначена для возможной беспроводной связи для автомобильной интеллектуальной транспортной системы (ITS)?
  - A. U-NII-1
  - B. U-NII-2A
  - C. U-NII-2B
  - D. U-NII-2C
  - E. U-NII-3
  - F. U-NII-4

- 12.** Когда данные повреждены предыдущими данными от отраженного сигнала, это называется как?
- A.** Разброс задержки (delay spread)
  - B.** Межсимвольная интерференция
  - C.** Со-канальная интерференция
  - D.** Интерференция смежных сот.
- 13.** Предполагая, что все каналы поддерживаются 5 ГГц точкой доступа, сколько возможных 20МГц каналов можно настроить на точке доступа?
- A.** 4
  - B.** 11
  - C.** 12
  - D.** 25
- 14.** Какая из этих технологий является наиболее устойчивой к негативным эффектам многолучевого распространения?
- A.** FHSS
  - B.** DSSS
  - C.** HR-DSSS
  - D.** OFDM
- 15.** Какое среднее количество агрегированной пропускной способности при любой скорости передачи данных, когда передают устаревшие радиомодули 802.11a/b/g/n/ac?
- A.** 80 процентов
  - B.** 75 процентов
  - C.** 50 процентов
  - D.** 100 процентов
- 16.** Какая из этих технологий 802.11 может работать в полосе частот 2,4ГГц? (Выберите все, что применимо)
- A.** 802.11a (радиомодули OFDM)
  - B.** 802.11b (радиомодули HR-DSSS)
  - C.** 802.11g (радиомодули ERP)
  - D.** 802.11n (радиомодули HT)
  - E.** 802.11ac (радиомодули VHT)
  - F.** 802.11ax (радиомодули HE)
- 17.** В Соединенных Штатах радиомодулям 802.11 не разрешено передавать в каком диапазоне частот для того, чтобы избежать интерференции с системами Доплеровского Метеорологического Радара (Terminal Doppler Weather Radar (TDWR))
- A.** 5.15 ГГц–5.25 ГГц
  - B.** 5.25 ГГц–5.25 ГГц
  - C.** 5.60 ГГц–5.65 ГГц
  - D.** 5.85 ГГц–5.925 ГГц

- 18.** Какие типы модуляции используются технологией OFDM? (Выберите все, что подходит).
- A.** QAM
  - B.** Фазовая
  - C.** Частотная
  - D.** Скачкообразная
- 19.** Коды Баркера конвертируют биты данных в серию битов, которые называются как?
- A.** Чипсеты (Chipsets)
  - B.** Чипы (Chips)
  - C.** Сверточный код
  - D.** Комплементарный код
- 20.** Какая технология будет нужна в U-NII-5 и U-NII-6 чтобы защитить точки доступа от интерференции с устройствами в 6 ГГц?
- A.** DFS
  - B.** AFC
  - C.** TPC
  - D.** QAM

# Глава

# 7



# Топологии Беспроводной ЛВС

**В ЭТОЙ ГЛАВЕ ВЫ УЗНАЕТЕ О  
СЛЕДУЮЩЕМ:**

✓ **Топологии беспроводных вычислительных сетей**

- Беспроводная вычислительная сеть широкого охвата (WWAN)
- Беспроводная городская вычислительная сеть (WMAN)
- Беспроводная персональная вычислительная сеть (WPAN)
- Беспроводная локальная вычислительная сеть (WLAN)

✓ **Станции 802.11**

- Станция-Клиент
- Станция-Точка Доступа
- Интеграционный сервис (IS)
- Система распространения (DS)
- Беспроводная система распространения (WDS)

✓ **Составы Сервиса 802.11**

- Идентификатор сервисного состава (SSID)
- Базовый состав сервиса (BSS)
- Область базового сервиса (BSA)
- Идентификатор состава базового сервиса (BSSID)
- Несколько идентификаторов состава базового сервиса
- Расширенный состав сервиса (ESS)
- Независимый базовый состав сервиса (IBSS)
- Персональный базовый состав сервиса (PBSS)



- Базовый состав сервиса с поддержкой взаимосвязности (MBSS)

- Базовый состав сервиса с поддержкой качества (QBSS)

✓ **Режимы настройки 802.11**

- Режимы точки доступа
- Режимы клиентской станции



Компьютерная (или вычислительная) сеть - это система, которая обеспечивает связь между компьютерами. Компьютерные сети могут быть настроены как равный-сравненный (peer-to-peer), клиент-сервер, или как кластеризованные центральные вычислительные блоки [CPUs] с распределенными простыми терминалами.

Сетевая *топология*[topology] определяется просто по физическому и/или логическому уровню узлов в компьютерной сети. Любой, кто проходил базовый курс по сетям, уже знаком с топологиями: шина (bus), кольцо(ring), звезда(star), взаимосвязанная(mesh) и гибридная, которые часто используются в проводных сетях.

Все топологии имеют свои преимущества и недостатки. Топология может покрывать очень маленькую область или существовать как всемирная архитектура. Беспроводные топологии также существуют как определяемые физическим или логическим уровнем беспроводного оборудования. Доступно много беспроводных технологий и они могут быть распределены по четырем основным беспроводным топологиям. Стандарт 802.11-2020 определяет один определенный тип беспроводной связи. В стандарте 802.11-2020 есть различные типы топологий, называемых как *составы сервиса* [service sets]. Годами, производители тоже использовали оборудование 802.11, использующее различные виды этих топологий, чтобы соответствовать конкретным потребностям беспроводных сетей. Эта глава охватывает топологии, используемые типовыми радиоволновыми технологиями и описывает топологии беспроводной локальной вычислительной сети (БЛВС) [Wireless LAN (WLAN)] специфичной для 802.11.

## Топологии Беспроводных Вычислительных Сетей

Хотя основной фокус этого учебного руководства - это беспроводная сеть 802.11, которая является технологией локальной области, существуют другие беспроводные технологии и стандарты, в которых беспроводная связь охватывает и небольшие территории, и огромные зоны покрытия. Примеры других беспроводных технологий включают в себя сотовую связь, Bluetooth, и Zigbee. Все эти различные беспроводные технологии можно разделить на следующие четыре основные беспроводные топологии:

- Беспроводная вычислительная сеть широкого охвата [Wireless wide area network - WWAN]
- Беспроводная городская вычислительная сеть [Wireless metropolitan area network – WMAN]
- Беспроводная персональная вычислительная сеть [Wireless personal area network – WPAN]
- Беспроводная локальная вычислительная сеть [Wireless local area network - WLAN или БЛВС]

Дополнительно, хотя стандарт 802.11-2020 - это БЛВС (или WLAN) стандарт, те же самые технологии могут иногда быть развернуты в других топологиях беспроводных сетей, как обсуждается в следующих разделах.

## Беспроводная вычислительная сеть широкого охвата

*Вычислительная сеть широкого охвата [wide area network (WAN)]* обеспечивает радиопокрытие на обширной географической территории. WAN может пересекать целые штаты, регионы или страны, или даже охватывать весь мир. Лучший пример WAN - это Интернет. Много частных и публичных корпоративных WAN состоит из аппаратной инфраструктуры, такой как линии T1 или E1, оптоволокно, и маршрутизаторы. Протоколы, используемые для проводной связи WAN включают: Ретрансляцию Кадров [Frame Relay], ATM, Многопротокольную Коммутацию Меток [Multiprotocol Label Switching (MPLS)], и другие.

*Беспроводная вычислительная сеть широкого охвата [wireless wide area network (WWAN)]* также охватывает широкие географические границы, но, очевидно, использует беспроводную среду вместо проводной среды. WWAN'ы обычно используют технологии сотовой телефонии или собственные лицензируемые технологии беспроводных мостов. Сотовые провайдеры, такие как AT&T Mobility (ЭйТи энд Ти Мобилити), Verizon (Верайзон), и Vodafone (Водафон), используют различные конкурирующие технологии для передачи данных. Некоторые примеры этих сотовых технологий - это сервис пакетной радиосвязи общего назначения [general packet radio service (GPRS)], множественный доступ с кодовым разделением [code division multiple access (CDMA)], множественный доступ с временным разделением [time division multiple access (TDMA)], Долгосрочная Эволюция [Long Term Evolution (LTE)], и Глобальная Система Мобильной Связи [Global System for Mobile Communications (GSM)]. Данные могут быть переданы различным устройствам, таким как смартфоны, планшеты, и сотовые USB модемы.

В прошлом, скорости передачи данных и ширина полосы, используемые этими технологиями были относительно медленными в сравнении с другими беспроводными технологиями, например: 802.11. Точно также как в Wi-Fi, скорости передачи данных были улучшены с развитием нескольких поколений сотовой технологии. Кроме того, конвергенция и сосуществование между технологией Wi-Fi и сотовой технологией становится реальностью.

## Беспроводная Городская Вычислительная Сеть

*Беспроводная городская вычислительная сеть [wireless metropolitan area network (WMAN)]* обеспечивает радиопокрытие городской территории, такой как город и окружающие пригороды. WMAN'ы некоторое время создавались различными подходящими беспроводными технологиями, а недавние улучшения сделали это более удобным. Одна беспроводная технология, которая наиболее часто ассоциируется с WMAN определена стандартом 802.16. Этот стандарт определяет широкополосный беспроводной доступ и иногда называется, как *Всемирная Совместимость для Микроволнового Доступа [Worldwide Interoperability for Microwave Access (WiMAX)]*. [произносится ВайМакс]. WiMAX Форум ответственен за тестирование на совместимость и совместную работоспособность оборудования беспроводного широкополосного доступа, такого как оборудование 802.16.

Технология 802.16 рассматривается как прямой конкурент другим широкополосным услугам, таким как DSL и кабельному подключению. Хотя беспроводная сеть 802.16 обычно считается как решение по организации последней мили для передачи данных, эта технология может также быть применена, чтобы обеспечить пользователям доступ по всему городу. На 2020 год,

в соответствии с консорциумом WiMAX Форума, существует 580 активных WiMAX сетей в 149 странах.



Больше информации о стандарте 802.16 можно найти по адресу <http://ieee802.org/16>. Узнайте больше о WiMAX на [www.wimaxforum.org](http://www.wimaxforum.org).

В прошлом, генерировалось много печатных материалов о возможности развертывания Wi-Fi сетей, покрывающих весь город и дающих горожанам доступ к сети Интернет на всей территории города. Хотя изначально технологию 802.11 никогда не предназначалось использовать для предоставления доступа на такой большой территории, у многих городов были инициативы, чтобы совершить этот подвиг. Оборудование, которое использовалось для этих крупномасштабных установок, было проприетарными беспроводными взаимосвязанными [mesh] маршрутизаторами или взаимосвязываемыми [mesh] точками доступа. Многие из этих городов отказались от своих первоначальных планов по развертыванию технологии 802.11 просто потому, что технология не могла масштабироваться на весь город. Однако, некоторые производители БЛВС имели партнерство с сервис провайдерами 4G/LTE, и имели успешные установки 802.11 WMAN с использованием 100000 точек доступа для городского доступа. Телекоммуникационные сервис провайдеры также начали использовать механизм, определенный в 802.11u, для разгрузки [offload] трафика данных сотовой связи в сети Wi-Fi.

## Беспроводная Персональная Вычислительная Сеть

*Беспроводная персональная вычислительная сеть [wireless personal area network (WPAN)]* это беспроводная компьютерная сеть, использующаяся для связи между компьютерными устройствами в непосредственной близости от пользователя. Устройства, такие как ноутбуки, игровые приставки, планшеты, и смартфоны могут связываться друг с другом, используя различные беспроводные технологии. WPANы могут быть использованы для связи между устройствами или в качестве портала к сетям более высокого уровня, таких как локальные вычислительные сети [local area networks (LANs)], и/или к сети Интернет. Наиболее распространенными технологиями в WPAN являются Bluetooth и инфракрасный свет. Инфракрасный свет - это среда на основе светового диапазона, в то время как Bluetooth - это среда радио диапазона, который использует технологию расширения спектра со скачкообразной перестройкой частоты (FHSS).

Рабочая Группа IEEE 802.15 фокусируется на технологиях, используемых для WPAN, таких как Zigbee и Bluetooth. Zigbee - это другая радиотехнология, которая имеет возможность создания недорогой беспроводной сети между устройствами в архитектуре WPAN.

IEEE 802.15.4 определяет работу низкоскоростных беспроводных персональных вычислительных сетей [low-rate wireless personal area networks (LR-WPANs)]. Почти также как стандарт 802.11-2020 определяет механизмы PHY и MAC для БЛВС, стандарт 802.15.4 определяет работу PHY и MAC для LR-PAN. Задача IEEE 802.15.4 обеспечить связь на дистанциях вплоть до 10 метров и со скоростью передачи данных 250кбит/с. Беспроводной Протокол Удаленного Датчика с Адресацией по Магистральной Шине [Wireless Highway Addressable Remote Transducer Protocol (WirelessHART)], это технология сети беспроводных датчиков, основанная на 802.15.4

*Zigbee* использует мало мощные радиомодули для оборудования автоматизации домов и промышленного оборудования, которому требуется беспроводная передача данных на короткое расстояние с небольшой скоростью. *IPv6 поверх Мало-Мощной Беспроводной Персональной Вычислительной Сети [IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN)]* определяет механизм передачи для IPv6 пакетов поверх сетей 802.15.4 WPAN.

*Тред[Thread] (в переводе с английского Нить)* - это маломощная взаимосвязанная [mesh] технология, используемая для IoT устройств, и которая построена поверх технологии 6LoWPAN. Тред(Нить) может подключить вплоть до 250 IoT устройств в беспроводной сети.



Вы можете найти больше информации о стандартах 802.15 WPAN на [www.ieee802.org/15](http://www.ieee802.org/15). Хотя изначально определенные IEEE в стандарте 802.15, стандарты Bluetooth сейчас находятся под присмотром Специальной Заинтересованной Группы Bluetooth (Bluetooth Special Interest Group (SIG)). Чтобы узнать больше о Bluetooth, посетите сайт [www.bluetooth.com](http://www.bluetooth.com). Альянс Zigbee предоставляет информацию о технологии Zigbee по адресу [www.zigbee.org](http://www.zigbee.org). Больше информации о Треде(Ните) можно найти на страничке альянса Тред Груп (Thread Group alliance) [www.threadgroup.org](http://www.threadgroup.org). Хотя фокус экзамена CWNA - это технология 802.11, программа CWNP также предлагает сертификацию - Сертифицированный Профессионал Беспроводных IoT Соединений. (Certified Wireless IoT Connectivity Professional (CWICP)), которая охватывает 802.15.4 и другие беспроводные технологии. Информация о CWICP доступна по адресу [www.cwnp.com/certifications/cwicp](http://www.cwnp.com/certifications/cwicp).

Производители Wi-Fi уровня предприятия производят точки доступа с радиомодулями 802.11, и некоторые из этих точек доступа включают радиомодули 802.15. Например, корпус точки доступа может содержать в себе два Wi-Fi радиомодуля для 2,4 и 5ГГц Wi-Fi связи, а также радиомодуль Bluetooth Низкой Энергии (*Bluetooth Low Energy (BLE)*) для задач в непосредственной близости. Решения для задач в непосредственной близости, использующие BLE, обсуждаются более детально в Главе 20, "Установки БЛВС и Вертикальные Рынки".

Мы предоставим информацию о сетях 802.11 равный-с-равным (peer-to-peer) позже в этой главе, в разделе "Независимый Базовый Сервисный Состав." Лучшим примером радиомодуля Wi-Fi 802.11, используемого в сценарии WPAN, будет соединение равный-с-равным (peer-to-peer). Технология компании Apple(эпл) - AirDrop(эйрдроп), которая работает поверх Bluetooth и Wi-Fi, является другим примером WPAN, используемым для передачи файлов между компьютерами или планшетами.

## Беспроводная Локальная Вычислительная Сеть

Как вы знаете из предыдущих глав, стандарт 802.11-2020 определен как технология беспроводной локальной вычислительной сети (*wireless local area network (WLAN)*). Локальные вычислительные сети обеспечивают образование сетей в зданиях или городках(кампусах). Беспроводная среда 802.11 идеально подходит для организации сетей, просто из-за охвата и скоростей, которые определены стандартом 802.11-2020 и будущими поправками. Большинство установок беспроводных сетей 802.11 являются действительно ЛВС, которые обеспечивают доступ на работе и дома.

Сети БЛВС обычно используют много точек доступа 802.11, подключенных проводной магистральной сетью. В установка на предприятиях, сети БЛВС

используются для обеспечения конечным пользователям доступа к сетевым ресурсам, и сетевым сервисам и шлюзу в Интернет. Хотя оборудование 802.11 может быть использовано в других беспроводных топологиях, основная часть установок Wi-Fi – это БЛВС, которые как технология изначально были определены Рабочей Группой 802.11 Института IEEE. Обсуждения БЛВС обычно относятся к решениям 802.11; однако существуют другие технологии собственной разработки и конкурирующие технологии БЛВС.

Пожалуйста, заметьте, что большие корпорации могут развернуть и управлять БЛВС 802.11 в глобальном масштабе. Wi-Fi сети предприятия с большим количеством мест географического присутствия может централизованно управляться, используя системы сетевого управления [network management system (NMS)] и могут также подключаться через виртуальные частные сети [virtual private networks (VPNs)]. Более глубокое обсуждение управления Wi-Fi сети, инфраструктуры и масштабируемости можно найти в Главе 11 «Архитектура БЛВС».

## Станции 802.11

Основной компонент беспроводной сети 802.11 – это радиомодуль, который называется стандартом 802.11 как *станция [station (STA)]*. Радиомодуль может находиться внутри точки доступа или использоваться в клиентской станции. Все станции определяются уникальным MAC [мак] адресом. Стандарт 802.11-2020 специфицирует архитектурные сервисы, которые станции используют внутри разных топологий 802.11. Есть три категории сервисов 802.11, которые работают на MAC подуровне 802.11:

**Станционный Сервис**      *Станционный сервис [station service (SS)]* присутствует во всех станциях 802.11, включая клиентские станции и точки доступа. Станционный сервис обеспечивает следующее:

- Аутентификацию [Authentication]
- Деаутентификацию [Deauthentication]
- Конфиденциальность данных
- Доставку MSDU
- Динамический выбор частоты (DFS)
- Контроль мощности передачи (TPC)
- Синхронизация таймеров более высокого уровня
- Диспетчеризация параметров качества(QoS) трафика
- Радиоизмерения
- Включение динамической станции (DSE)

Хотя эти сервисы станции работают на подуровне MAC, многое также зависит от информации с Физического уровня. Например, радиомодули с поддержкой DFS обнаруживают импульсы радара по физической радио среде, но используют обмен 802.11 MAC кадров для оповещений о переключении канала. Большой объем этих клиентских сервисов обсуждается значительно детальнее в различных главах этой книги.

**Сервис Системы Распространения**      *Сервис системы распространения [distribution system service (DSS)]* работает только внутри точек доступа и

взаимосвязанных [mesh] порталах. DSS используется для управления ассоциациями, повторными ассоциациями, деассоциациями (разъединением) и т.д. со станцией-клиентом. Более детальное обсуждение DSS следует далее в этой главе.

**Сервис Контрольной Точки PBSS** Сервис контрольной точки PBSS (*PBSS control point service (PCPS)*) определен специально для радиомодулей 802.11ad при работе в очень специфичной топологии 802.11, называемой персональный базовый состав сервиса (PBSS), который обсуждается позже в этой главе. PCPS управляет ассоциациями, повторными ассоциациями, деассоциациями, и диспетчеризацией качества (QoS) трафика при развертывании топологии PBSS.

## Станция-Клиент

Любой радиомодуль, который не используется в точке доступа, обычно называется, как *станция-клиент*, или *клиентская станция [client station]* или станция не точка-доступа [non-AP station]. Радиомодули станции-клиента могут быть использованы в ноутбуках, планшетах, сканерах, смартфонах, и многих других мобильных устройствах. Радиомодули станций-клиентов могут также быть использованы в стационарном оборудовании таком как настольные компьютеры и устройства IoT. Станции-клиенты должны бороться за полудуплексную радиосреду таким же способом, что и точка доступа. Когда станции-клиенты имеют соединение на 2 уровне с точкой доступа, они называются *ассоциированными (associated)*. Ассоциировавшись, станции -клиенты могут воспользоваться преимуществами функциональности портала, которую предоставляет точка доступа. Хотя, станции-клиенты 802.11 могут быть стационарными, предполагается, что они мобильны и могут поддерживать связь при переключении (роуминге) между точками доступа. Все станции-клиенты поддерживают станционные сервисы.

## Станция-Точка Доступа

Станция-точка доступа (ТД) [*access point (AP)*] 802.11 – это радиомодуль, который функционирует как беспроводной портал, через который другие клиентские станции могут соединяться. В общем, точка доступа имеет всю ту же самую функциональность, что и станция-клиент. Однако, ключевое различие между станцией-точкой доступа и станцией-клиентом – это функциональность портала. Точка доступа предоставляет функциональность портала, позволяя ассоциированным станциям-клиентам устанавливать связь из беспроводной среды в другую физическую среду, такую как сеть Ethernet 802.3. Технический термин этой функциональности портала – *функция доступа к системе распространения [distribution system access function (DSAF)]*.

Как ранее говорилось, точки доступа также используют сервис системы распространения (DSS) для управления клиентскими ассоциациями. Хорошей аналогией будут таблицы контентно-адресуемой памяти [*content-addressable memory (CAM)*] в управляемом коммутаторе. Под контентом подразумевается содержание Ethernet кадра. Управляемый проводной коммутатор управляет динамическими таблицами MAC[мак] адресов, называемых *таблицы CAM[кам] [CAM tables]*, которые направляют кадры в порты на основе MAC адресов назначения кадра. Аналогично, точка доступа управляет *таблицей ассоциаций [association table]* подключенных Wi-Fi клиентов, и направляет трафик.

## Интеграционный Сервис

Стандарт 802.11-2020 определяет, что *интеграционный сервис [integration service*

(IS)] делает возможным передачу MSDU между системой распространения(DS) и не-IEEE 802.11 ЛВС через портал. Более простой способ определения сервиса интеграции — это охарактеризовать ее как способ передачи формата кадра. Портал — это обычно точка доступа или БЛВС контроллер. Полезная нагрузка кадра данных беспроводного стандарта 802.11 – информация уровней 3-7 называется, как блок данных *MAC[мак] сервиса [MAC service data unit (MSDU)]*. Финальный пункт назначения этой полезной нагрузки обычно проводная сетевая инфраструктура. Так как проводная инфраструктура - это другая физическая среда, полезная нагрузка кадра данных 802.11 должна быть фактически перенесена в кадр Ethernet 802.3. Например, VoWiFi телефон посыпает кадры данных 802.11 отдельно стоящей точке доступа. Полезная нагрузка MSDU кадра – VoIP пакет с конечным пунктом назначения – IP АТС (IP PBX), которая располагается в ядре сети 802.3. Работа интеграционного сервиса – убрать заголовок и окончание 802.11 и поместить полезную нагрузку VoIP MSDU в кадр 802.3. Кадр 802.3 затем отправляется в сеть Ethernet. Интеграционный сервис выполняет те же самые действия в обратном случае, когда полезная нагрузка кадра 802.3 должна быть перенесена в кадр 802.11, который в итоге модулируется и передается радиомодулем точки доступа.

Определение того, как работает интеграционный сервис находится за пределами стандарта 802.11-2020. Обычно интеграционный сервис переносит полезную информацию кадра данных между 802.11 и 802.3 средами. Однако, интеграционный сервис может переносить MSDU между средой 802.11 и некоторыми видами других сред. Если пользовательский трафик 802.11 направляется на границу сети, интеграционный сервис находится на точке доступа. Обычно интеграционный сервис имеет место быть внутри БЛВС контроллера, когда пользовательский трафик 802.11 туннелируется до БЛВС контроллера.

## Система Распространения

Как ранее упоминалось, ключевая разница между радиомодулями точек доступа 802.11 и станциями-клиентами – это функциональность портала точки доступа. Эта характеристика портала также называется функцией доступа системы распространения (DSAF). Стандарт 802.11-2020 определяет систему распространения, которая используется, чтобы соединить ряд базовых сервисных составов через встроенную ЛВС, чтобы создать расширенный сервисный состав(ESS). Сервисные составы детально описаны позже в этой главе. Точки доступа по своей природе являются устройствами-порталами. Беспроводной трафик может быть направлен обратно в беспроводную среду или направлен в интеграционный сервис. DS состоит из следующих двух основных компонентов:

**Среда Системы Распространения** Логическая физическая среда, используемая для подключения точек доступа, называется *средой системы распространения [distribution system medium (DSM)]*. Наиболее общий пример - это физическая среда 802.3, также известная как Ethernet.

**Сервис Системы Распространения** Как обсуждалось ранее, сервис системы распространения(DSS) используется в точках доступа, чтобы управлять ассоциациями, повторными ассоциациями и деассоциациями клиентских станций. Сервис системы распространения также использует адресацию 2 уровня MAC заголовка, чтобы в итоге переслать информацию уровней 3-7 (MSDU) или в интеграционный сервис или другой беспроводной клиентской станции. Полное понимание DSS находится за пределами границ экзамена CWNA.

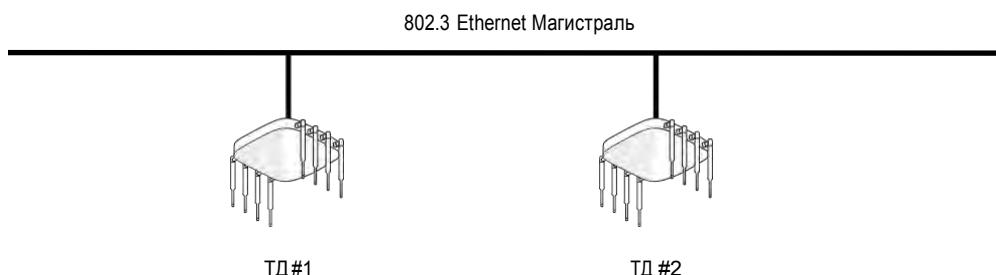
Одиночная точка доступа или несколько точек доступа могут быть подключены к одной и

той же среде системы распространения. Большая часть установок 802.11 использует точку доступа в качестве портала в 802.3 Ethernet магистраль, которая работает как среда системы распространения. Точки доступа обычно подключены к коммутируемой Ethernet сети, которые часто предлагают выгодную опцию подачи питания на точку доступа с помощью технологии Электропитание по Ethernet (Power over Ethernet (PoE)).

Точка доступа может также действовать как устройство-портал в другую проводную и беспроводную среды. Стандарт 802.11-2020 по плану не заботиться и не определяет в какую среду точка доступа конвертирует и пересыпает данные. Следовательно, точка доступа может быть охарактеризована как конвертирующий мост [*translational bridge*] между двумя средами. Точка доступа конвертирует и пересыпает данные между средой 802.11 и любой другой средой, используемой средой системы распространения. Еще раз, среда системы распространения почти всегда будет 802.3 Ethernet сеть, как показано на рисунке 7.1. В случае беспроводной взаимосвязной [mesh] сети - обычно это пересылка через серию беспроводных устройств, с конечным пунктом назначения 802.3 сеть.

### Р И С У Н О К 7.1

### Среда системы распространения



## Беспроводная Система Распространения

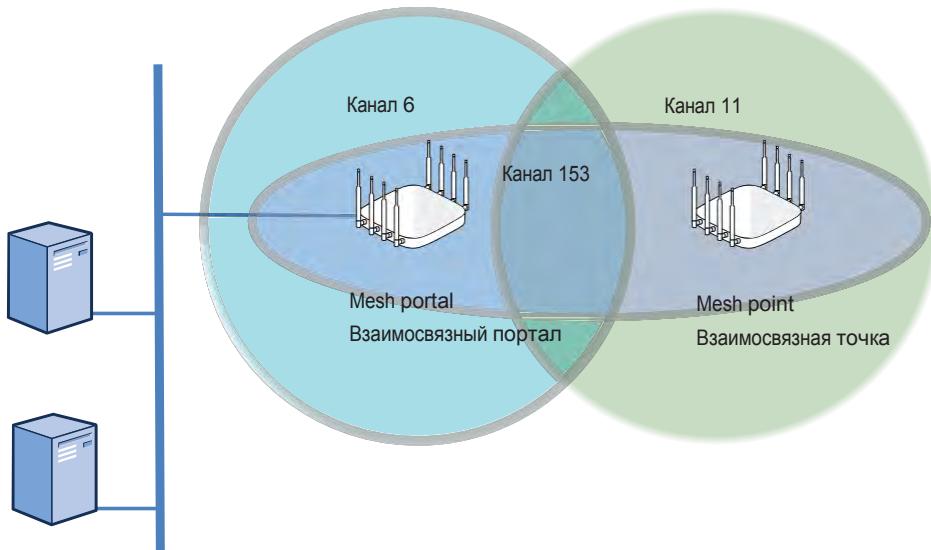
Стандарт 802.11-2020 определяет механизм для беспроводной связи, используя формат кадра, содержащий четыре MAC адреса. Стандарт описывает такой формат кадра, но не описывает как такой механизм или формат кадра нужно использовать. Этот механизм называется беспроводной система распространения [*wireless distribution system (WDS)*]. Хотя DS обычно использует проводную Ethernet магистраль, однако вместо нее возможно использовать и беспроводное соединение. WDS может соединить две точки доступа вместе, используя, что называется, беспроводной транзитный канал [*wireless backhaul*]. Как изображено на Рисунке 7.2, наиболее обычный для реального мира пример WDS - это когда точки доступа работают во взаимосвязной(mesh) сети, чтобы обеспечить покрытие и магистраль (опорную сеть). Как показано на Рисунке 7.3, еще один реальный пример WDS - это уличный канал связи типа мост 802.11, используемый для обеспечения беспроводной магистральной связи между двумя зданиями. Более детальное обсуждение о сетях с поддержкой взаимосвязности [mesh] сетях и БЛВС мостах можно найти в нескольких главах в этой книге.

### Какая Система Распространения Наиболее Желательна?

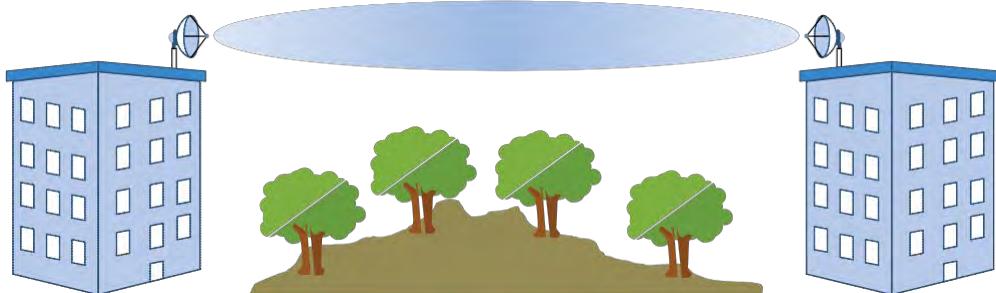
Проводная сеть обычно является лучшим вариантом для системы распространения. Потому что на большинстве установок на предприятии на местах уже есть проводная 802.3 инфраструктура, и интеграция беспроводной сети в Ethernet сеть является наиболее логичным решением. Среда проводной системы распространения не встречает множества проблем, которые могут повлиять на WDS, например, как

физическое препятствие или радио интерференция. Многосвязная(mesh) магистральная(backhaul) сеть иногда является более лучшим вариантом, когда есть сложности с прокладкой кабеля. Дополнительно, внешний канал связи типа 802.11 мост может быть единственным вариантом для соединения двух зданий или строений. Если возникает ситуация, когда проводная сеть не может соединить точки доступа вместе, то WDS может быть реальной альтернативой. Более желаемое решение WDS использует разные частоты и радиомодули для клиентского доступа и распространения.

**Р И С У Н О К 7.2**      Беспроводная система распространения - транзитный канал во взаимосвязной [mesh] сети



**Р И С У Н О К 7.3**      беспроводной мост



# Составы Сервиса 802.11

Стандарт 802.11-2020 определяет несколько топологий, называемых *составами сервиса [service sets]*, которые описывают как эти радиомодули могут быть использованы, чтобы связываться друг с другом. Эти топологии 802.11 называются как базовый состав сервиса [basic service set (BSS)], расширенный состав сервиса [extended service set (ESS)], независимый базовый состав сервиса [independent basic service set (IBSS)], персональный базовый состав сервиса [personal basic service set (PBSS)], базовый состав сервиса с поддержкой взаимосвязности [mesh basic service set (MBSS)], и базовый состав сервиса с поддержкой качества [QoS basic service set (QBSS)]. В следующих разделах мы опишем все компоненты, из которых состоят различные сервисные составы 802.11.

## Идентификатор Сервисного Состава

*Идентификатор сервисного состава [service set identifier (SSID)]* - это логическое имя, используемое для идентификации беспроводной сети 802.11. Имя SSID беспроводной сети сравнимо с именем рабочей группы в Windows. Радиомодули используют это логическое имя в нескольких различных обменах кадрами 802.11. SSID - это настраиваемый параметр на всех радиомодулях 802.11, включая точки доступа и клиентские станции. SSID может состоять из вплоть до 32 символов, и чувствителен к регистру. Рисунок 7.4 показывает настройку SSID на точке доступа.

**Р И С У Н О К 7 . 4** Идентификатор сервисного состава

Wireless Network		
Name (SSID) *	Sybex Wi-Fi	Broadcast SSID Using
Broadcast Name *	Sybex Wi-Fi	<input checked="" type="checkbox"/> WiFi0 Radio (2.4 GHz or 5 GHz) <input checked="" type="checkbox"/> WiFi1 Radio (5 GHz only)

Большинство точек доступа имеют возможность скрытия SSID и держать сетевое имя скрытым от нелегитимных конечных пользователей. Скрытие SSID является слабой и ошибочной попыткой в безопасности, которая неопределена стандартом 802.11-2020. Однако, этот вариант ошибочно выбирается некоторыми администраторами.

Для того, чтобы клиенты незаметно(бесшовно) переключались, точки доступа должны вещать один и тот же SSID, настроенный с одними и теми же настройками безопасности.



Скрытие SSID обсуждается в Главе 17, "Архитектура Сетевой Безопасности 802.11"

## Базовый Состав Сервиса

*Базовый состав сервиса [basic service set (BSS)]* является фундаментальной топологией сети 802.11. Устройства связи, которые образуют BSS, это радиомодуль одной точки доступа с одной или несколькими станциями-клиентами. Клиентские станции присоединяются к беспроводному домену точки доступа, и начинают обмениваться данными через точку доступа. Станции, которые являются членами BSS, имеют соединение 2 уровня и называются *ассоциированной или связанной[associated]*. Рисунок 7.5 изображает стандартный базовый состав сервиса.

Обычно ТД подключена к среде системы распространения, но это не является требованием базового состава сервиса. Если ТД работает как портал в систему распространения, клиентские станции связываются через ТД с сетевыми ресурсами, которые находятся в DSM. В реальном мире цель BSS – это иметь связь через ТД с сетевыми ресурсами и доступ к шлюзу в Интернет для Wi-Fi клиентов.

**Р И С У Н О К 7 . 5** Базовый состав сервиса



Основная связь по БЛВС является клиент-серверной. Однако, если клиентские станции 802.11 захотят обмениваться данными напрямую друг с другом, они пересыпают свои

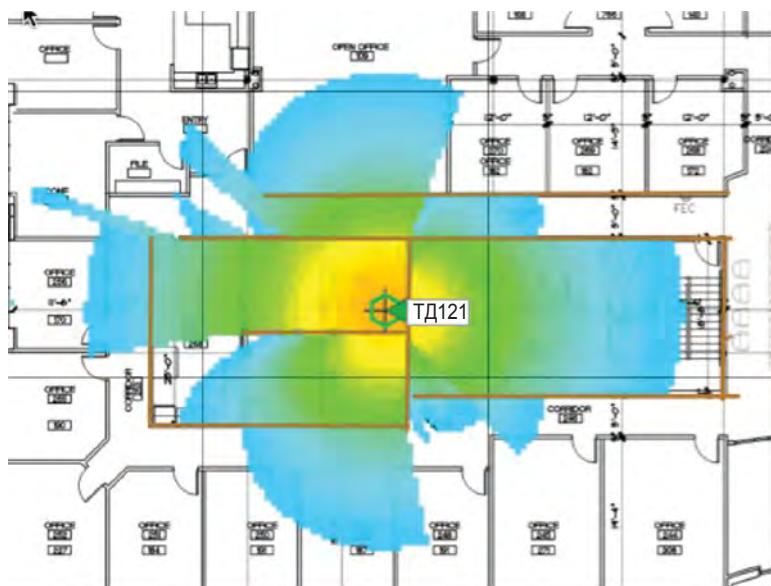
данные через точку доступа. В типовом BSS, связь равный-с-равным от одной клиентской станции к другой клиентской станции может продолжаться до тех пор, пока трафик пересыпается через точку доступа. Клиенты, которые поддерживают установку туннелированного прямого канала связи [*tunneled direct link setup (TDLS)*] являются редким исключением из этого правила. Клиенты с TDLS могут обмениваться данными прямо друг с другом и в обход точки доступа. TDLS клиенты остаются ассоциированными (соединенными) с точкой доступа, и по-прежнему участвуют в качестве клиента BSS. Наоборот, большинство производителей БЛВС предлагают функционал изоляции клиентов [*client isolation*], чтобы блокировать связь равный-с-равным между клиентами ассоциированными с точкой доступа.

Вы можете увидеть другую терминологию 802.11, используемую для описания базового состава сервиса. Например, VHT BSS относится к базовому составу сервиса в точке доступа 802.11ac. DMG BSS состав сервиса относится к базовому составу сервиса в точке доступа 802.11ad.

## Область Базового Сервиса

Физическая область покрытия, предоставляемая точкой доступа BSS называется *областью базового сервиса [basic service area (BSA)]*. Рисунок 7.6 показывает типичную BSA. Клиентские станции могут перемещаться по области покрытия и поддерживать связь с точкой доступа до тех пор, пока принимаемый сигнал между радиомодулями остается выше порогов индикатора силы принимаемого сигнала (RSSI). Радиомодули клиентских станций и Точек доступа могут также переключаться между концентрическими зонами переменных скоростей передачи данных, которые есть в BSA. Процесс перемещения по скоростям передачи данных называется динамическое переключение скоростей передачи данных, и обсуждается в Главе 13 "Концепции Проектирования БЛВС"

**РИСУНОК 7.6** Область базового сервиса



Размер и форма BSA зависит от многих переменных, включая мощность передачи ТД, усиления антенны, приемной чувствительности, и физического окружения. Так как окружающая среда и физическое окружение часто изменяются, BSA часто может быть изменчивой. Когда рисуешь BSA, обычно рисуешь круг вокруг ТД, чтобы проиллюстрировать теоретическую область покрытия. Реально область покрытия будет иметь непропорциональную форму из-за существующей среды внутри и снаружи помещений. Вы также можете добавить, что фактическое расстояние и форма BSA определяются только с точки зрения любой подключенной клиентской станции, поскольку все клиентские устройства интерпретируют RSSI по-разному.

## Идентификатор Базового Состава Сервиса

48 битный (6 октетный) MAC адрес радиомодуля точки доступа называется *идентификатором базового состава сервиса [basic service set identifier (BSSID)]*. Простое определение BSSID это то, что это MAC адрес сетевого радиоинтерфейса в точке доступа. Однако, правильное определение - это то, что адрес BSSID является идентификатором 2 уровня каждого отдельного BSS.

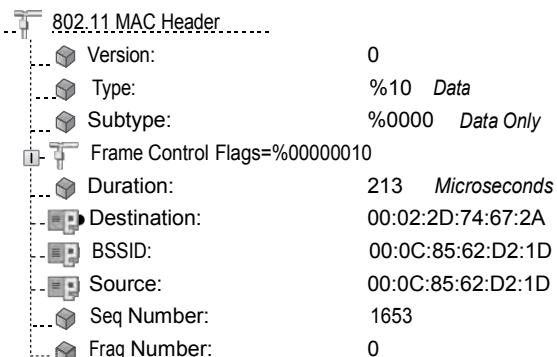
В предыдущем разделе вы узнали, что базовый состав сервиса состоит из ТД с одной или более станциями, ассоциированными с ТД. Если два состава базового сервиса находятся рядом друг с другом, и оба вещают один и тот же SSID, клиентской станции нужно как-то различать один BSS от другого. Для того, чтобы клиенты бесшовно переключались, точки доступа обязаны вешать один и тот же SSID, настроенный с одними и теми же параметрами безопасности. Клиентской станции, однако, все еще нужно видеть уникальный идентификатор 2 уровня каждой ТД, чтобы переключаться (осуществлять роуминг). BSSID обеспечивает каждый BSS уникальным идентификатором, то есть именем BSSID. Термин *смена BSS [BSS transition]* относится к процессу роуминга клиентской станции, перемещающейся из одного BSS в другой BSS.



Не путайте адрес BSSID с SSID. Идентификатор состава сервиса (SSID) – это логическое имя БЛВС, которое настраивается пользователем, в то время как BSSID – это MAC адрес 2ого уровня радиомодуля, присвоенный производителем оборудования.

Как показано на Рисунке 7.7, адрес BSSID находится в заголовке MAC большинства беспроводных кадров 802.11, и используется для целей идентификации базового состава сервиса. Адрес BSSID играет роль в направлении трафика 802.11 внутри базового состава сервиса. Помните, что адрес BSSID используется как уникальный идентификатор 2 уровня базового состава сервиса, и является критичным для процесса роуминга.

**Р И С У Н О К 7.7** Идентификатор базового состава сервиса



## Несколько Идентификаторов Базового Состава Сервиса

Как вы уже знаете, каждый БЛВС имеет логическое имя (SSID), и каждый BSS БЛВС имеет уникальный идентификатор 2 уровня (BSSID). BSSID может быть физическим MAC адресом радиомодуля точки доступа; однако, может быть создано несколько BSSID для радиоинтерфейса, используя подинтерфейсы, как показано на Рисунке 7.8. Несколько BSSID обычно увеличивают оригинальный MAC адрес радиомодуля ТД.

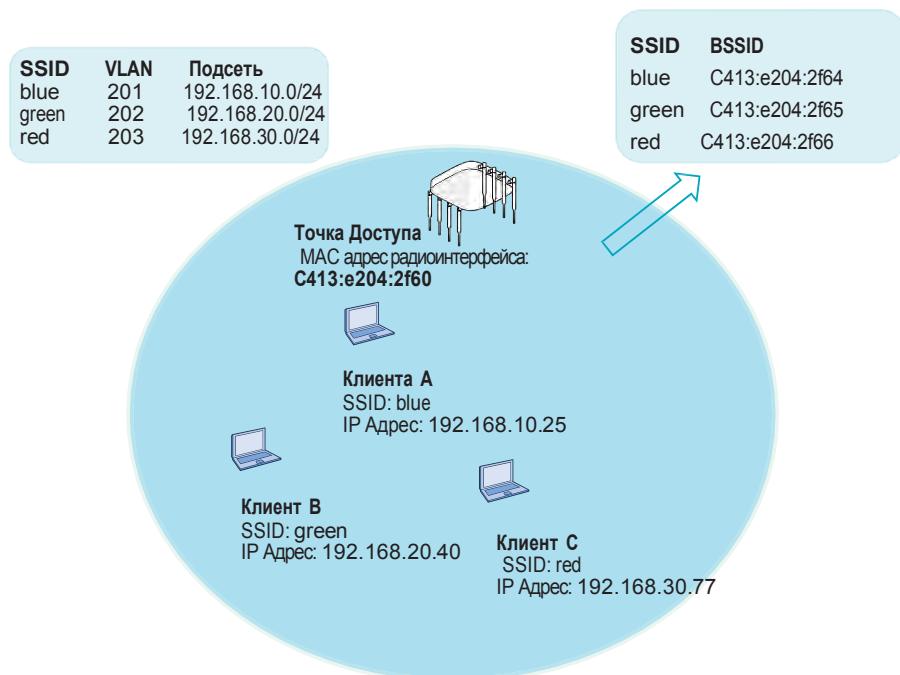
**Р И С У Н О К 7.8** Увеличивающиеся адреса BSSID

Name	MAC addr	SSID	Chan(Width)
Wifi1	c413:e204:2f60		48(20MHz)
Wifi1.1	c413:e204:2f64	green	48(20MHz)
Wifi1.2	c413:e204:2f65	blue	48(20MHz)
Wifi1.3	c413:e204:2f66	red	48(20MHz)

Если радиоинтерфейс ТД имеет MAC адрес, зачем вам нужно несколько BSSID, а не просто использовать MAC адрес ТД в качестве идентификатора на 2 уровне? Причина в том, что производители Wi-Fi уровня предприятия предоставляют средства для точек доступа поддерживать несколько БЛВС одновременно.

Как показано на Рисунке 7.9, несколько БЛВС могут существовать внутри каждой зоны покрытия точки доступа. Каждая БЛВС имеет уникальное логическое имя (SSID) и уникальный идентификатор на 2 уровне (BSSID), и каждый SSID обычно привязан к уникальной виртуальной локальной вычислительной сети (VLAN), которая привязана к уникальной подсети (Здесь уровня). Другими словами, несколько доменов уровней 2/3 могут существовать внутри одного домена 1ого уровня. Попробуйте представить несколько составов базового сервиса, которые связаны с несколькими VLAN`ами, при этом они все существуют внутри одной и той же зоны покрытия одной точки доступа.

**Р И С У Н О К 7 . 9**      Несколько идентификаторов базового состава сервиса (BSSIDs)



### Пример из Реальной Жизни

#### Будут ли Влиять на Производительность Несколько SSID и BSSID?

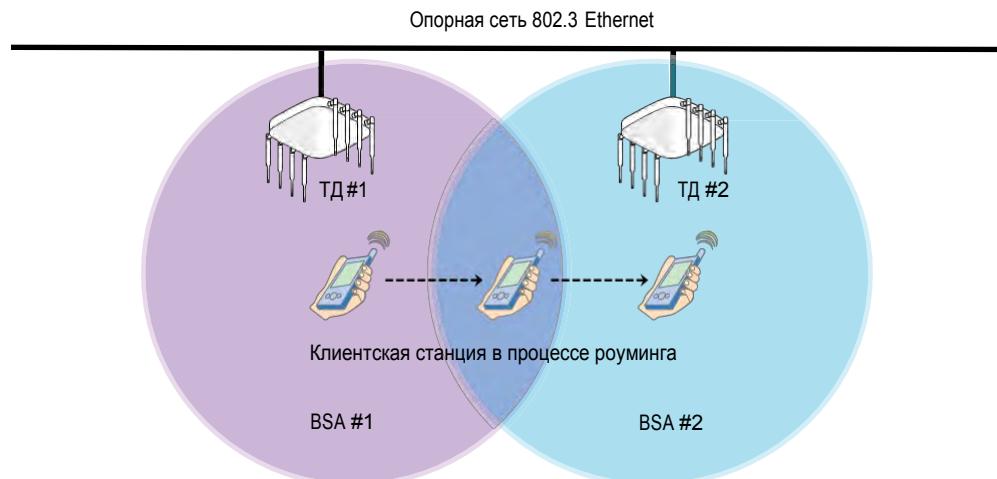
Простой ответ – да, если есть слишком много SSID, передающихся с одного и того же радиоисточника точки доступа. При создании нескольких SSID, существование нескольких базовых составов сервиса (BSS) приводит к избыточному количеству служебной информации (накладных расходов) MAC уровня. Многие производители Wi-Fi уровня предприятия поддерживают передачу 16 SSID и фактически 16 BSS с радиомодуля одной точки доступа. Идентифицированный уникальным BSSID каждый базовый состав сервиса

будет иметь свою собственную служебную информацию (собственные накладные расходы), состоящую из набора маяков, ответов на зондирование, и других кадров управления и контроля. Если радиомодуль одной точки доступа передает 16 маяков (beacons) с интервалом 100 мс каждый, то создается экстремальное количество дополнительных накладных расходов на MAC уровне, что приводит к серьезным проблемам в производительности. Из-за этого потенциального ухудшения производительности, большинство инженеров-проектировщиков БЛВС рекомендуют вещать не более трех или четырех SSID.

## Расширенный Состав Сервиса

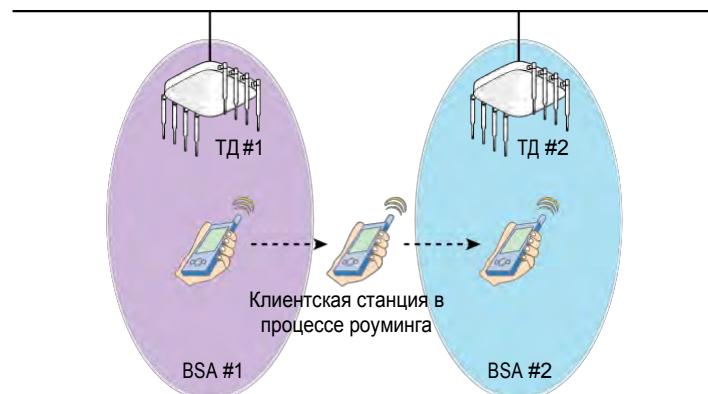
В то время как BSS может считаться краеугольным камнем топологии 802.11, то топология *расширенного состава сервиса [extended service set (ESS)]*, по аналогии - целое каменное здание. Расширенный состав сервиса это две или более одинаково настроенных базовых составов сервиса, соединенных средой системы распространения. Обычно расширенный состав сервиса - это набор нескольких точек доступа и их ассоциированных(присоединенных) клиентских станций, объединенных единой DSM. *Область расширенного сервиса [extended service area (ESA)]* это область покрытия ESS, в которой все клиенты могут обмениваться данными и переключаться между точками. Наиболее типовой пример ESS состоит из точек доступа с перекрывающимися зонами, как показано на Рисунке 7.10. Целью ESS с перекрывающимися зонами покрытия - обеспечить бесшовный роуминг клиентским станциям. Перекрытие покрытия действительно дублирует покрытие с точки зрения Wi-Fi станции-клиента и обсуждается более подробно в Главе 13.

**Р И С У Н О К 7.10**      Расширенный состав сервиса, бесшовный роуминг



Хотя незаметный(бесшовный) роуминг обычно является ключевым аспектом проекта БЛВС, нет таких требований к ESS, чтобы гарантировать непрерывную связь. Например, ESS может использовать несколько точек доступа с неперекрывающимися зонами покрытия, как показано на Рисунке 7.11. В этом сценарии, станция клиент, которая покидает область базового сервиса (BSA) первой точки доступа потеряет связь. Позже клиентская станция переустановит соединение, как только она попадет в зону покрытия второй точки доступа. Этот способ мобильности станции между несоприкасающимися зонами иногда называется, как *кочующий роуминг [nomadic roaming]*.

**РИСУНОК 7.11** Расширенный состав сервиса, кочующий роуминг



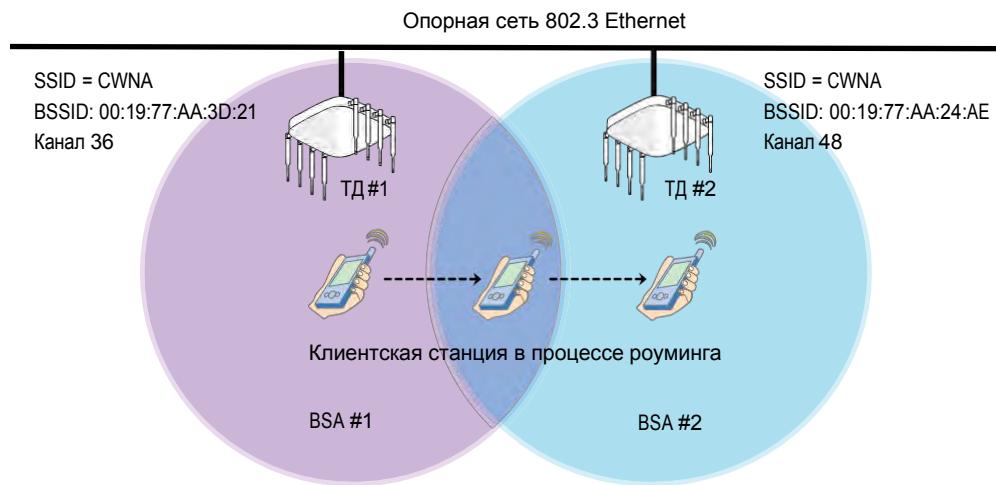
Заметьте, что оба примера только что упомянутых расширенных составов сервиса имеют общую систему распространения. Как утверждалось ранее в этой главе, обычно среда системы распространения - это 802.3 Ethernet сеть; однако, DS может использовать другой тип среды. В расширенном составе сервиса точки доступа используют одно и то же имя SSID. Логическое сетевое имя ESS часто называется *идентификатор расширенного состава сервиса [extended service set identifier (ESSID)]*. Термины ESSID и SSID являются синонимами. Как иллюстрирует Рисунок 7.12, точки доступа в ESS, где требуется роуминг, все должны использовать одно и то же логическое имя (SSID) и настройки безопасности, но они должны иметь уникальные идентификаторы 2 уровня (BSSID) для каждой уникальной зоны покрытия BSA.

## Независимый Базовый Состав Сервиса

Третья топология сервисного состава, определенная стандартом 802.11, - это *независимый базовый состав сервиса [independent basic service set (IBSS)]*.

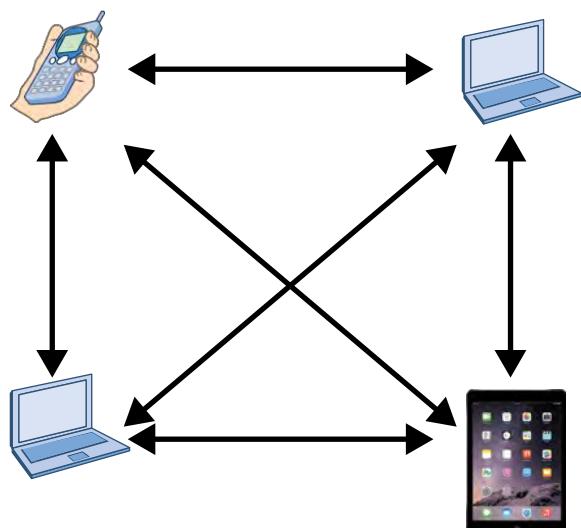
Радиомодули, которые образуют сеть IBSS, являются только клиентскими станциями (STAs) без какой-либо установленной точки доступа. Сеть IBSS, которая состоит только из двух STA является аналогом проводного кроссового кабеля. IBSS может, однако, иметь несколько клиентских станций в одной физической области общающихся в специальном для этого случая режиме – режиме ad hoc или «на лету». Рисунок 7.13 изображает четыре клиентские станции обменивающихся данными друг с другом в режиме равный-с-равным.

Р И С У Н О К 7.12 SSID и BSSID внутри ESS



Все станции передают кадры друг другу напрямую и не маршрутизируют кадры от одного клиента к другому клиенту. Весь обмен кадров клиентских станций в IBSS является равный-с-равным. Все станции в IBSS должны бороться за полудуплексную среду, и в любое выбранное время только одна STA может быть передающей.

Р И С У Н О К 7.13 Независимый базовый состав сервиса





Независимый базовый состав сервиса имеет два других имени. Производители Wi-Fi часто называют IBSS или как сеть равный-с-равным [*peer-to-peer network*], или как сеть «на лету» (*ad hoc network*).

Для того, чтобы связь IBSS была успешна, все станции должны передавать на одном и том же частотном канале. Более того, этот весь набор отдельных беспроводных станций, соединенных вместе в группу, должны использовать одно и тоже имя SSID БЛВС. Еще одно замечание об IBSS это то, что создается адрес BSSID. Ранее в этой главе, мы определили BSSID как MAC адрес радиомодуля внутри точки доступа. Так, как может независимый базовый состав сервиса иметь BSSID, если не используется ни одной точки доступа в топологии IBSS? Первая станция, которая стартует в IBSS случайным образом генерирует BSSID в формате MAC адреса. Этот случайным образом сгенерированный BSSID является виртуальным MAC адресом, и используется для целей идентификации 2 уровня внутри IBSS. На заре Wi-Fi, редактируемые настройки режима «на лету» (*ad hoc*) на клиентских устройствах были обычным делом; однако, функционал IBSS не поддерживается широко в современных клиентских устройствах.

## Персональный Базовый Состав Сервиса

Аналогично IBSS, *персональный базовый состав сервиса [personal basic service set (PBSS)]* является топологией 802.11 БЛВС, в которой станции 802.11ad общаются напрямую друг с другом. PBSS может быть установлен только радиомодулями *направленного мультигигабита [directional multi-gigabit (DMG)]*, которые передают в 60ГГц полосе частот. Аналогично IBSS, тут нет централизованной точки доступа, которая работает как портал в среду системы распространения, такую как проводная сеть 802.3 Ethernet. В отличие от IBSS, один клиент берет на себя роль *контрольной точки PBSS [PBSS control point (PCP)]*. Клиент PCP использует кадры DMG Маяк (Beacon) и Анонс(Announce) чтобы обеспечить синхронизированный доступ к среде между всеми клиентами, участвующими в PBSS.

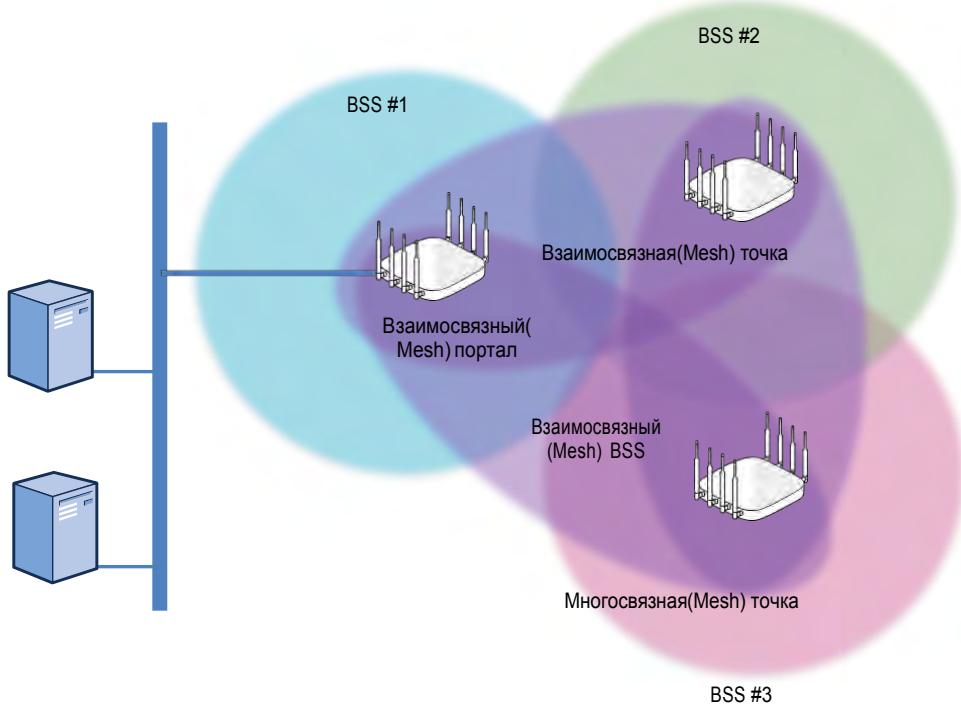
Как ранее утверждалось, PBSS может быть установлена только радиомодулями совместимыми с 802.11ad, которые передают на частоте 60ГГц. Следует отметить, что радиомодули DMG могут также обмениваться данными с другими радиомодулями DMG через топологии BSS или IBSS.

## Базовый Состав Сервиса с Поддержкой Взаимосвязности

Стандарт 802.11 имеет давно определенные составы сервиса BSS, ESS, и IBSS. Стандарт 802.11-2020 также определяет сервисный состав для взаимосвязной [*mesh*] топологии 802.11. Когда точки доступа поддерживают функции взаимной связности [*mesh*], они могут быть установлены там, где невозможен проводной сетевой доступ. Функции взаимной связности [*mesh*] используются, чтобы предоставить беспроводное распределение сетевого трафика, а набор точек доступа, которые обеспечивают взаимосвязное [*mesh*] распределение формируют *базовый состав сервиса с поддержкой взаимосвязности [mesh basic service set (MBSS)]*. MBSS требует свойства, которые не нужны в BSS, ESS или IBSS, потому что назначение MBSS отличается от других топологий. Как показано на Рисунке 7.14, одна или более точек доступа обычно

подключены к проводной инфраструктуре. Любая ТД с поддержкой взаимосвязности [mesh], подключенная к вышестоящей проводной среде называется *взаимосвязанным порталом или mesh- порталом [mesh portal]*. Технический термин в 802.11 для станции взаимосвязного портала [mesh- портала] - взаимосвязанный шлюз [mesh gate или mesh gateway]. Любые другие взаимосвязанные [mesh] точки доступа, которые не подключены к проводной сети будут образовывать беспроводные транзитные [backhaul] соединения к взаимосвязанным [mesh] порталам, чтобы достичь проводной сети. Взаимосвязанные [mesh] точки доступа, которые не подключены к вышестоящей проводной инфраструктуре называются взаимосвязанными точками или mesh точками [mesh points, или MPs]. Транзитные соединения между взаимосвязанной [mesh] точкой и взаимосвязанным [mesh] порталом считаются беспроводной системой распространения [wireless distribution system (WDS)]. Клиентские станции, которые ассоциированы с взаимосвязанной [mesh] точкой должны направлять свой трафик через беспроводной транзитный канал [backhaul]. Обычно MBSS используют 5 ГГц радиомодули для транзитной связи.

**Р И С У Н О К 7.14** Взаимосвязанный базовый состав сервиса



Взаимосвязанные узлы [mesh nodes] в MBSS функционируют почти как маршрутизаторы в сети, потому что их цель обнаружить соседние взаимосвязанные [mesh] станции, определить возможные и наилучшие соединения до портала, сформировать каналы с соседями, и поделиться информацией о каналах. Держите в уме, что обмен кадрами 802.11 является операцией 2 уровня; следовательно, взаимосвязанная [mesh] маршрутизация трафика 802.11 базируется на MAC адресах, а не на IP адресах. *Гибридный беспроводной взаимосвязанный протокол [hybrid wireless mesh protocol (HWMP)]* определен как протокол выбора пути по-умолчанию для MBSS. HWMP является и проактивным, и

реактивным, и фактически является динамическим протоколом маршрутизации 2 уровня. Заметьте, что производители Wi-Fi предлагают функции взаимосвязности [mesh] много лет, используя собственный взаимосвязанные [mesh] протоколы 2 уровня. Из-за конкуренции стандартная версия HWRP не поддерживается производителями Wi-Fi уровня предприятия. Они продолжают использовать свои собственные динамические механизмы 2 уровня, используя такие метрики как RSSI, SNR, клиентская загрузка, и количество пролетов [hop], чтобы определить лучший путь для транзитного [backhaul] трафика. Инфраструктура БЛВС, используемая для обеспечения взаимосвязной сетевой работы БЛВС, уже прошла несколько поколений, которые обсуждаются в Главе 11.

## Базовый Состав Сервиса с поддержкой качества(QoS)

Механизмы качества сервиса [*quality of service (QoS)*] могут быть внедрены во все сервисные наборы 802.11. Улучшения Качество Сервиса [QoS] доступны станциям с QoS [QoS STAs], ассоциированными с точкой доступа с QoS [QoS access point] в базовом составе сервиса с QoS [QoS BSS]. Станции с QoS также могут принадлежать одному и тому же независимому базовому составу сервиса с QoS [QoS IBSS]. Старые радиомодули, которые не поддерживают механизмы QoS, называются *станциями без поддержки QoS [non-QoS STAs и non-QoS APs]*. Глава 8, “802.11 Доступ к Среде,” обсуждает механизмы QoS более детально. Механизмы QoS требуются при сертификации Wi-Fi Мультимедиа [Wi-Fi Multimedia (WMM)], которые строго проверяются Wi-Fi Альянсом. Любая точка доступа 802.11 уровня предприятия, произведенная за последние 12 лет, поддерживает механизмы WMM QoS по умолчанию. Следовательно, каждый базовый состав сервиса в большинстве установок на предприятиях считается *базовым составом сервиса с поддержкой QoS [QoS basic service set (QBSS)]*.



### Реальный Сценарий

#### Выбор Производителя При Развёртывании и Интеграции инфраструктуры БЛВС 802.11

При развертывании инфраструктуры 802.11, рекомендуемая практика - это приобретение оборудования от одного производителя. Маловероятно, что мост от производителя А будет работать с мостом от производителя Б. Взаимосвязанная[mesh] точка от производителя А наиболее вероятно не будет обмениваться данными с взаимосвязанным [mesh] порталом от производителя Б. Другой пример маловероятной взаимной работоспособности - это переключение между точками доступа разных производителей при роуминге. Клиентские станции могут быть не способны эффективно переключаться между точками доступа при использовании Wi-Fi точек доступа разных производителей.

Главное назначение ТД 802.11 - выступать в качестве портала в проводную сетевую инфраструктуру. Хотя технология 802.11 работает на уровнях 1 и 2, всегда существуют вопросы проектирования более высокого уровня. Все производители БЛВС имеют разные стратегии о том, как интегрироваться в существующую проводную сетевую инфраструктуру. По этой причине нормальный наилучший подход - это придерживаться одного производителя БЛВС для предприятий при развертывании и интеграции инфраструктуры 802.11.

# Режимы настройки 802.11

В то время как стандарт 802.11-2020 определяет все радиомодули как станции (STA), радиомодуль точки доступа и радиомодуль клиентской станции могут быть настроены многочисленными способами. Заводская настройка радиомодуля ТД позволяет работать в базовом составе сервиса(BSS) в качестве портала в проводную сетевую инфраструктуру. Однако, ТД может быть настроена, чтобы работать и в других режимах работы. Некоторые клиентские станции могут быть настроены так, чтобы участвовать в BSS или IBSS составе сервиса 802.11.

## Режимы Точки Доступа

Заводская настройка точек доступа некоторых производителей БЛВС называется *корневым режимом [root mode]*. Основное назначение ТД - работать в качестве портала в распределительную систему. Обычные заводские настройки ТД - это корневой режим, который позволяет ТД передавать данные в обе стороны между DS и беспроводной средой 802.11. Не все производители используют эти же названия для этого режима работы. Например, большинство производителей Wi-Fi используют термин *режим ТД [AP mode]* или *режим доступа [access mode]* вместо корневого режима.

Заводская настройка радиомодуля ТД позволяет работать в качестве беспроводного портала BSS. Существуют, однако, другие рабочие режимы, в которые можно настроить ТД.

**Режим Взаимосвязности [Mesh]** Радиомодуль ТД работает в качестве транзитного [backhaul] беспроводного радиомодуля во взаимосвязной [mesh] среде. В зависимости от производителя, радиомодуль для транзитного канала может также поддерживать и клиентский доступ. *Взаимосвязанный режим [Mesh mode]* иногда также называется, как *режимом повторителя [repeater mode]*.

**Режим Сенсора** Радиомодуль ТД переключается в радиосенсор, позволяя ТД интегрироваться в архитектуру беспроводной системы обнаружения проникновения (WIDS). ТД в режиме сенсора находится в состоянии непрерывного прослушивания, сканируя несколько каналов. *Режим сенсора [Sensor mode]* также часто называют *режимом мониторинга [monitor mode]* или *режимом сканера [scanner mode]*.

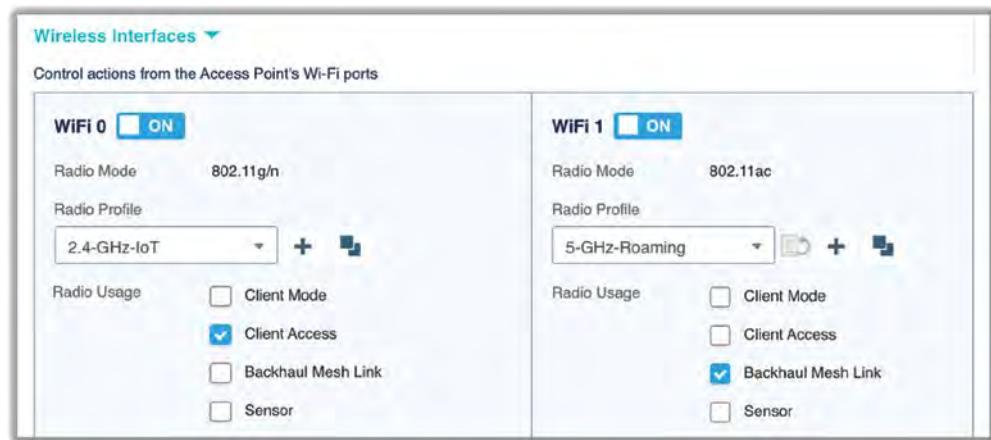
**Режим Моста** ТД переключается в беспроводной мост. Это обычно добавляет устройству дополнительный интеллект на MAC уровне, и дает ТД способность изучать и управлять таблицей MAC адресов со стороны проводной сети.

**Режим Моста Рабочей Группы** Радиомодуль ТД трансформируется в мост рабочей группы, обеспечивающий беспроводную магистраль для подключенных проводных 802.3 клиентов.

**Режим ТД в качестве Клиента** ТД работает как клиентское устройство, которое может ассоциироваться с другой ТД. Этот режим работы иногда используется в целях поиска и устранения проблем.

Стандарт 802.11-2020 не определяет эти режим работы ТД; следовательно, каждый производитель Wi-Fi будет иметь разные возможности. Эти режимы работы являются «режимами настройки радиомодуля» и может быть применена к радиомодулю 2,4ГГц в ТД, радиомодулю 5ГГц в ТД, или обоим радиомодулям. Производители Wi-Fi часто используют различную терминологию для различных доступных режимов настройки. На Рисунке 7.15 вы можете посмотреть пример настраиваемые режимы ТД одного производителя.

**Р И С У Н О К 7.15** Режимы настройки точки доступа



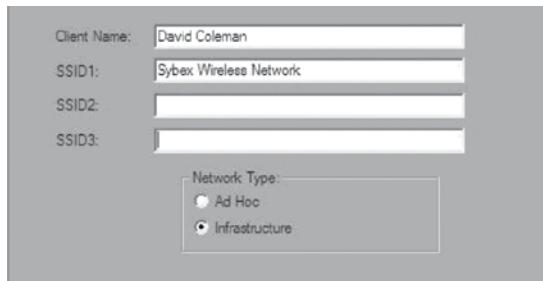
## Режимы Клиентской Станции

Клиентская станция может работать в одном из двух состояний, как показано на Рисунке 7.16. Заводской режим клиентского радиомодуля 802.11 обычно *инфраструктурный режим* [*infrastructure mode*]. Работая в режиме инфраструктуры, клиентская станция позволяет осуществлять передачу данных через точку доступа. Инфраструктурный режим позволяет клиентской станции участвовать в базовом составе сервиса или расширенном составе сервиса. Клиенты, которые настроены на этот режим, могут обмениваться данными через ТД с другими беспроводными клиентскими станциями внутри BSS. Этот клиентский режим часто не заметен, потому что у клиентских устройств этот режим работы установлен по умолчанию, так что клиенты могут просто обнаружить точки доступа.

Клиенты могут также обмениваться данными через ТД с другими сетевыми устройствами, которые присутствуют в системе распространения, такие как сервера или проводные настольные устройства.

Второй режим клиентской станции называется *режимом "на лету"* [*ad hoc mode*]. Некоторые производители клиентов могут называть этот режим как *режим равный-сравненным* [*peer-to-peer mode*]. Клиентские станции 802.11, установленные в режим "на лету" (*ad hoc*), участвуют в топологии IBSS и не обмениваются данными через точку доступа. Все передачи станций и обмен кадрами являются одноранговыми (т.е. равный-сравненные). Много клиентских станций, таких как планшеты и смартфоны, могут не иметь настройки "режима на лету" [*ad hoc*].

**Р И С У Н О К 7.16** Режимы настройки клиентской станции



## Итого

Эта глава охватывает основные типы общих беспроводных топологий, а также топологии характерных для беспроводной сети 802.11:

- Четыре беспроводных архитектуры, которые могут быть использованы многими различными беспроводными технологиями
- Составы сервиса 802.11, определенные стандартом 802.11-2020, и различные аспекты и назначения, определенные для каждого сервисного состава.
- Режимы работы точек доступа и клиентских станций

Как администратор беспроводной сети вам следует полностью понимать определенные составы сервиса 802.11 и как они работают. Администраторы обычно следят за дизайном и управлением 802.11 ESS, но есть хорошая вероятность, что они также будут устанавливать радиомодули 802.11, используя и другие режимы работы.

## Темы Экзамена

**Знать четыре основных типа беспроводных топологий.** Понимать различия между WWAN, WLAN, WPAN, и WMAN.

**Объяснить различные составы сервиса 802.11** Быть способным полностью объяснить все компоненты, назначение и различия базового состава сервиса, расширенного состава сервиса, независимого базового состава сервиса, персонального базового состава сервиса, базового состава сервиса с поддержкой качества, базового состава сервиса с поддержкой взаимосвязности. Понимать как радиомодули 802.11 взаимодействуют друг с другом в каждом составе сервиса.

**Идентифицировать различные варианты, в которых может быть использован радиомодуль 802.**

Понимать, что стандарт 802.11 ожидает, что радиомодуль будет использован в качестве клиентской станции или внутри точки доступа. Также понимать, что радиомодуль 802.11 может быть использован по другому назначению, например как мост, для поддержки взаимосвязности(mesh) и т.д.

**Объяснить назначение системы распространения.** Знать, что DS состоит из двух частей: сервисы системы распространения (DSS) и среды системы распространения (DSM). Понимать, что среда, используемая DS, может быть средой любого типа. Объяснить работу беспроводной системы распространения (WDS).

**Дать определение SSID, BSSID, и ESSID.** Быть способным объяснить различия и сходства всех трех терминов и работу каждого.

**Описать различные варианты, в которых может быть применен ESS и назначение каждой схемы.** Объяснить три варианта, в которых зоны покрытия точек доступа ESS могут быть спроектированы, и назначение каждой схемы.

**Объяснить режимы работы точки доступа и клиентской станции.** Вспомните все режимы работы ТД и клиентской станции.

## Контрольные Вопросы

1. Логическое имя беспроводной сети 802.11 называется, как какой тип адреса? (Выберите все, что применимо.)

  - A. BSSID
  - B. MAC адрес
  - C. IP адрес
  - D. SSID
  - E. ESSID
2. Какие две топологии 802.11 требуют использование ТД?

  - A. IBSS
  - B. BSS
  - C. PBSS
  - D. ESS
3. Стандарт 802.11 определяет какую среду для использования в распределительной системе?

  - A. 802.3 Ethernet
  - B. 802.4 Token bus
  - C. 802.5 Token ring
  - D. 802.8 Fiber optic
  - E. 802.16 WiMAX
  - F. Ничего из выше перечисленного
4. Какой вариант является беспроводной компьютерной топологией, используемой для связи между компьютерными устройствами в непосредственной близости от пользователя?

  - A. WWAN
  - B. WMAN
  - C. WLAN
  - D. WPAN
5. Какой состав сервиса 802.11 облегчает роуминг для клиентских Wi-Fi устройств?

  - A. ESS
  - B. BSS
  - C. IBSS
  - D. PBSS

6. Какой фактор может повлиять на размер области базового сервиса? (Выберите все, что применимо.)
- A. Усиление антенны
  - B. CSMA/CA
  - C. Мощность передачи
  - D. Окружение снаружи/внутри помещений
  - E. Распределительная система
7. Учитывая, что многие производители Wi-Fi уровня предприятия поддерживают передачу нескольких SSID и, фактически, нескольких BSS с одного радиомодуля ТД, какие из этих утверждений являются верными? (Выберите все, что применимо.)
- A. При создании нескольких SSID, существование нескольких составов базового сервиса (BSS) приводит к избыточному количеству служебной информации MAC уровня.
  - B. Максимальное число SSID и соответствующих базовых наборов сервиса на передающий радиомодуль равно 8.
  - C. При создании нескольких SSID, существование нескольких базовых составов сервиса (BSS) обеспечивает больше эфирного времени (airtime) и большую производительность.
  - D. Максимальное число SSID и соответствующих базовых составов сервиса на передающий радиомодуль равно 16.
  - E. Максимальное число SSID и соответствующих базовых составов сервиса на передающий радиомодуль зависит от производителя.
8. Какой термин описывает топологию 802.11, содержащую STA, но не содержащую точки доступа? (Выберите все что применимо.)
- A. BSS
  - B. "На лету" (Ad hoc)
  - C. DSSS
  - D. Инфраструктура (Infrastructure)
  - E. IBSS
  - F. Равный-с-равным (Peer-to-peer)
9. Клиентские STA 802.11, работающие в инфраструктурном режиме по-умолчанию (или с заводскими настройками инфраструктурного режима), в обычной BSS могут обмениваться данными в каком из следующих сценариев? (Выберите все, что применимо.)
- A. Обмен кадрами 802.11 с другими клиентскими STA 802.11 через ТД
  - B. Обмен кадрами 802.11 TDLS прямо с другими клиентскими STA в BSS'ах.
  - C. Обмен кадрами 802.11 IBSS прямо с другими клиентскими STA в BSS
  - D. Обмен кадрами с сетевыми устройствами в DSM
  - E. Все вышеперечисленное

- 10.** Что из перечисленного включено в топологии, определенные стандартом 802.11-2020? (Выберите все, что применимо)
- A.** DSSS
  - B.** ESS
  - C.** BSS
  - D.** IBSS
  - E.** FHSS
  - F.** PBSS
- 11.** Какая беспроводная топология обеспечивает всегородское беспроводное покрытие?
- A.** WMAN
  - B.** WLAN
  - C.** WPAN
  - D.** WAN
  - E.** WWAN
- 12.** На каком уровне модели OSI используется адрес BSSID?
- A.** Физический [Physical]
  - B.** Сетевой [Network]
  - C.** Сеансовый [Session]
  - D.** Канальный [Data-Link]
  - E.** Прикладной [Application]
- 13.** Адрес BSSID может быть найден в какой топологии? (Выберите все, что применимо)
- A.** FHSS
  - B.** IBSS
  - C.** ESS
  - D.** HR-DSSS
  - E.** BSS
- 14.** Какой состав сервиса 802.11 определяет механизм для взаимосвязной [mesh] работы сети?
- A.** BSS
  - B.** PBSS
  - C.** ESS
  - D.** MBSS
  - E.** IBSS
- 15.** Какой состав сервиса 802.11 определен специально для направленного мультигигабита (DMG)?
- A.** BSS
  - B.** ESS

- C. IBSS
- D. PBSS
- E. MBSS

16. Стандарт 802.11-2020 определяет архитектурные сервисы, которые станции используют внутри различных топологий. Какой сервис используется и клиентскими станциями и станциями точками доступа?

- A. Сервис станции [Station service]
- B. Сервис распространения [Distribution service]
- C. Сервис контрольной точки PBSS [PBSS control point service]
- D. Интеграционный сервис [Integration service]
- E. Сервис шины [Bus service]

17. Сеть, состоящая из клиентов и двух точек доступа с одним и тем же SSID и соединенных опорной сети 802.3 Ethernet, является примером какой топологии 802.11? (Выберите все, что применимо.)

- A. Публичный базовый состав сервиса
- B. Базовый состав сервиса
- C. Расширенный состав сервиса
- D. Независимый базовый состав сервиса
- E. Ethernet состав сервиса

18. Какой термин лучше всего описывает две точки доступа общающиеся друг с другом беспроводно, в то же время позволяя клиентам передавать данные через точку доступа?

- A. WDS
- B. DS
- C. DSS
- D. DSSS
- E. DSM

19. Какие компоненты образуют систему распространения? (Выберите все, что применимо.)

- A. HR-DSSS
- B. DSS
- C. DSM
- D. DSSS
- E. QBSS

20. Какой тип беспроводной топологии определен стандартом 802.11-2020?

- A. WAN
- B. WLAN
- C. WWAN
- D. WMAN
- E. WPAN



# Глава 8



## Доступ к Среде 802.11

---

**В ЭТОЙ ГЛАВЕ ВЫ УЗНАЕТЕ  
СЛЕДУЮЩЕЕ:**

- ✓ **CSMA/CA против CSMA/CD**
  - Обнаружение конфликтов
- ✓ **Функция Распределенной Координации (DCF)**
  - Контроль физической несущей
  - Контроль виртуальной несущей
  - Псевдослучайный таймер отсрочки
  - Межкадровое пространство
- ✓ **Функция Гибридной Координации (HCF)**
  - Расширенный Распределенный Доступ к Каналам (EDCA)
  - Доступ к Каналу, Контролируемый Функцией Гибридной Координации (HCCA)
- ✓ **Wi-Fi Мультимедиа (WMM)**
- ✓ **Справедливость Эфирного Времени**



Одна из сложностей, которая у нас была во время написания этой главы, это то, что для того, чтобы вы поняли, как беспроводная станция получает доступ к среде, мы должны рассказать больше, чем это нужно для экзамена CWNA. Подробности нужны, чтобы понять концепции; однако, концепции - это то, на что вы будете проверяться на экзамене.

Если вы решите сдать экзамен Сертифицированный Профессионал по Анализу Беспроводных сетей (Certified Wireless Analysis Professional (CWAP)), то в это время вам нужно будет знать подробности, выходящие далеко за рамки того, что мы включили в эту главу. Но сейчас, примите подробности за то, чем они являются: фундаментом, который поможет вам понять весь процесс того, как беспроводная станция получает доступ к полудуплексной среде.

## CSMA/CA против CSMA/CD

Сетевая связь требует набора правил для обеспечения контролируемого и эффективного доступа к сетевой среде. *Контроль Доступа к Среде [Medium access control (MAC)]* является общим термином, используемым при обсуждении концепции доступа. Существует много способов обеспечения доступа к среде. Первые майнфреймы использовали опрашивание [polling], которое последовательно проверяло каждый терминал, чтобы узнать есть ли там данные для обработки. Позже, для предоставления доступа к среде использовались методы передачи токенов или передачи жетонов (token-passing) и методы конкурентного доступа или борьбы. Две формы конкурентного доступа, которые больше всего используются в сегодняшних сетях это *Множественный Доступ с Контролем Несущей и Обнаружением Конфликтов [Carrier Sense Multiple Access with Collision Detection (CSMA /CD)]* и *Множественный Доступ с Контролем Несущей и Предотвращением Конфликтов [Carrier Sense Multiple Access with Collision Avoidance (CSMA /CA)].*

CSMA/CD хорошо известен и используется для 802.3 Ethernet. БЛВС 802.11 используют менее известный CSMA/CA для доступа к среде. Станции, использующие любой из этих методов доступа, должны сначала послушать, чтобы определить вещает ли какое-либо устройство; и если так, станция должна подождать пока среда станет доступной. Разница между CSMA/CD и CSMA/CA находится в точке, когда клиент готов начать передачу и никакие другие клиенты на текущий момент не передают.

Проводные узлы CSMA/CD сначала проверяют передает ли какой-либо другой узел. Если никакой другой проводной клиент не передает в среде Ethernet, то узел отправляет первый бит информации. Если конфликт не обнаружен, узел продолжает посыпать другие биты информации, при этом непрерывно проверяя обнаружен ли конфликт. Если конфликт обнаружен, проводной узел вычисляет случайное количество времени, чтобы подождать, прежде чем начать процесс снова. Беспроводные радиомодули 802.11 не могут передавать и принимать в одно и то же время, поэтому они не способны обнаружить конфликт во время своей передачи. По этой причине, беспроводные сети 802.11 используют CSMA/CA вместо CSMA/CD, чтобы постараться избежать коллизии (конфликта).

Когда станция CSMA/CA определила, что никакая другая станция не осуществляет передачу, радиомодуль 802.11 выбирает случайным образом значение обратного отсчета [backoff]. Затем станция ждет дополнительное время, основанное на этом значении обратного таймера [backoff], прежде чем передавать. В течении этого времени, станция продолжает следить (мониторить), чтобы убедиться, что никакая другая станция не начала передачу. Из-за полудуплексной природы радиосреды, необходимо убедиться, что в любое выбранное время только один радиомодуль 802.11 контролирует среду. CSMA/CA - это процесс, используемый, чтобы удостовериться, что только один радиомодуль 802.11 передается в одно и тоже время. Является ли этот процесс совершенным? Абсолютно нет! Конфликты (или коллизии) продолжают случатьсяся, когда два или более радиомодуля передают в одно и то же время.

Стандарт IEEE 802.11-2020 определяет функцию, называемую *Функция Распределенной Координации [Distributed Coordination Function (DCF)]*, которая позволяет автоматически делить среду между совместимыми PHY (физическими уровнями устройств) путем использования протокола CSMA/CA. Также DCF с выгодой использует ACK (подтверждающие) кадры в качестве метода, подтверждающего доставку. CSMA/CA использует несколько проверок и противовесов, чтобы постараться минимизировать конфликты. Эти проверки и противовесы могут также рассматриваться как несколько линий обороны. Различные линии обороны размещаются в надежде, чтобы снова, гарантировать, что только один радиомодуль передает, пока все другие радиомодули слушают. CSMA/CA минимизируют риск конфликтов без избыточной служебной информации. Дополнительно, стандарт 802.11-2020 содержит Функцию Гибридной Координации [Hybrid Coordination Function (HCF)], которая специфицирует улучшенные методы качества сервиса [*quality-of-service (QoS)*].

Весь этот процесс раскрыт более детально в следующих разделах этой главы.

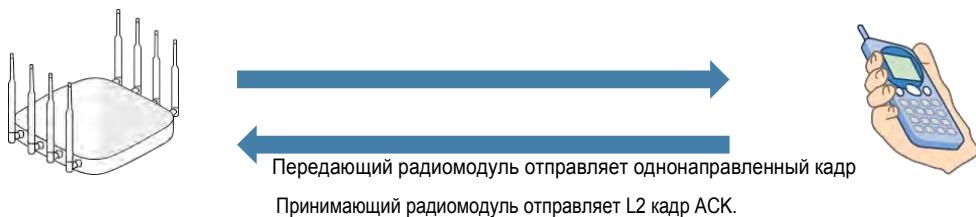
### Обзор CSMA/CA

Контроль несущей [Carrier sense] определяет занята ли среда. Множественный доступ [Multiple access] гарантирует, что каждому радиомодулю будет дан честный выстрел в среду (но только одному одновременно). Предотвращение конфликтов [Collision avoidance] означает, что только один радиомодуль получает доступ к среде в любое выбранное время, в надежде, избежать конфликтов.

## Обнаружение конфликтов

В предыдущем разделе, мы упомянули, что радиомодули 802.11 не могут передавать и принимать в одно и то же время, а следовательно не могут обнаружить конфликты (коллизии). Таким образом, если они не могут обнаружить конфликт, как они узнают случился и он? Ответ прост. Как показано на Рисунке 8.1, каждый раз радиомодуль 802.11 передает односторонний [unicast] кадр, если кадр получен правильно, то радиомодуль 802.11, который получил кадр, ответит кадром подтверждения [acknowledgment (ACK)]. Кадр ACK frame - это способ подтверждения доставки односторонних кадров.

Радиомодули 802.11n, 802.11ac, and 802.11ax используют агрегацию кадров, которая объединяет несколько односторонних кадров. Доставка агрегированных кадров подтверждается использованием Блока подтверждений [Block ACK].



Основная часть уникастовых кадров 802.11 должна быть подтверждена.

Широковещательные [broadcast] и многовещательные [multicast] кадры не требуют подтверждения. Если какая-либо часть однонаправленного кадра повреждена, то циклическая избыточная проверка [cyclic redundancy check (CRC)] провалится, и принимающий радиомодуль 802.11 не отправит ACK кадр передающему радиомодулю 802.11. Если кадр ACK не получен изначально передающим радиомодулем, то однонаправленный [unicast] кадр - не подтвержден, и должен быть отправлен повторно.

Этот процесс не определяет точно случился ли конфликт - другими словами, здесь нет обнаружения конфликта. Однако, если кадр ACK не получен первоначальным радиомодулем, то есть предположение о конфликте. Считайте ACK кадр способом подтверждения доставки однонаправленного кадра 802.11. Если подтверждение о доставке не предоставлено, то первоначальный радиомодуль делает предположение, что доставка не удалась, и отправляет этот кадр повторно.

## Функция Распределенной Координации

*Функция Распределенной Координации [Distributed Coordination Function (DCF)]* - это фундаментальный метод доступа связи 802.11, а процесс CSMA/CA является фундаментом DCF. С добавлением поправки 802.11e, которая теперь является частью стандарта 802.11-2020, расширенная координационная функция, называемая как *Функция Гибридной Координации [Hybrid Coordination Function (HCF)]* строится далее на методах доступа DCF. В следующих разделах вы узнаете о некоторых компонентах, которые являются частью процесса CSMA/CA. Здесь четыре главные компоненты протокола CSMA/CA, в соответствии с определением DCF:

- Физический контроль несущей [Physical carrier sense ]
- Виртуальный контроль несущей [Virtual carrier sense ]
- Псевдо-случайный обратный таймер [Pseudo-random backoff timer ]
- Межкадровое пространство [Interframe spaces ]

Радиомодули 802.11 используют механизмы контроля несущей, чтобы определить занята ли беспроводная среда. Представьте себе это как, прослушивание сигнала занято, когда звоните кому-то. Существует два способа, которыми осуществляется контроль несущей: физический контроль несущей и виртуальный контроль несущей. Радиомодули 802.11 борются за среду, используя псевдо-случайный алгоритм и обратный таймер, прежде чем осуществить передачу. Межкадровые пространства также используются для большего обеспечения уровней приоритета для доступа к беспроводной среде.

Думайте об этих четырех компонентах как о проверках и противовесах, которые работают вместе в одно и то же время, чтобы гарантировать, что только один радиомодуль 802.11 передает в полу-дуплексной среде. Эти четыре компонента будут объяснены отдельно, но важно понимать, что все четыре механизма работают в одно и то же время.

## Физический Контроль Несущей

CSMA/CA использует линии обороны, чтобы гарантировать, что станция не передает, пока другая уже передает: стандарт 802.11-2020 определяет механизм *физического контроля несущей [physical carrier sense]* для определения занята ли радиоволновая среда.

Физический контроль несущей выполняется постоянно всеми станциями, которые не осуществляют передачу или прием. Когда станция выполняет физический контроль несущей, она в действительности слушает канал, чтобы увидеть занимает ли какая-либо другая радиопередача данный канал.

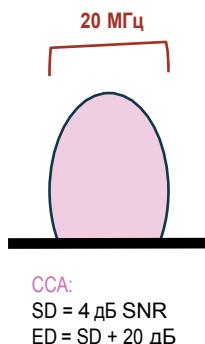
Физический контроль несущей имеет два назначения:

- Первое назначение – определить является ли передача кадра входящей для станции, чтобы осуществить прием. Если среда занята, радиомодуль будет пытаться синхронизоваться с передачей.
- Второе назначение – определить является ли среда занятой, прежде чем передавать. Среда должна быть чистой, прежде чем станция может вести передачу.

Чтобы достичь эти двух целей физического контроля несущей, радиомодули 802.11 используют *проверку чистого канала [clear channel assessment (CCA)]*, чтобы оценить радиосреду. Проверка чистого канала (CCA) включает в себя прослушивание радио передач на Физическом уровне. Радиомодули 802.11 используют два отдельных порога CCA при прослушивании радиосреды. Как показано на Рисунке 8.2, порог *обнаружения сигнала [signal detect (SD)]* используется, чтобы идентифицировать любую преамбулу 802.11 передачи от других передающих радиомодулей 802.11. Преамбула – это компонент заголовка Физического уровня передачи кадра 802.11. Преамбула используется для синхронизации между передающим и принимающим радиомодулями 802.11. Порог SD иногда называется *порогом преамбулы контроля несущей [preamble carrier sense threshold]*. Порог обнаружения сигнала по статистике равен 4dB отношения сигнала-шум (SNR) для большинства радиомодулей 802.11, чтобы обнаружить и декодировать преамбулу 802.11. Другими словами, радиомодуль 802.11 может обычно декодировать преамбулу 802.11 любой входящей передачи при принимаемом сигнале около 4dB выше уровня шума.

**РИСУНОК 8.2**

Проверка чистого канала (CCA)



Порог *Обнаружение Сигнала (SD)* по статистике равен 4 dB отношения сигнал-шум, чтобы обнаружить преамбулу 802.11.

Порог *Обнаружения Энергии (ED)* на 20 dB больше над порогом обнаружения сигнала.

CCA:

SD = 4 dB SNR

ED = SD + 20 dB

Порог обнаружения энергии [energy detect (ED)] используется для обнаружения любого другого типа радио передач во время процесса проверки чистого канала (CCA). Помните, что полосы 2,4 ГГц и 5ГГц являются полосами не требующими лицензий, и другие не-802.11 радиопередачи могут занимать канал. Как показано на Рисунке 8.2, порог ED на 20 дБ выше, чем порог обнаружения сигнала. Например, если уровень шума канала 36 был -95 дБм, порог SD для обнаружения передачи 802.11 будет около -91 дБм, и порог ED для обнаружения других радиопередач будет -71 дБм. Если уровень шума канала 40 был -100 дБм, порог SD по обнаружению передачи 802.11 был бы около -96 дБм, и порог ED по обнаружению других радиопередач был бы -76 дБм.

Примерно 4 микросекунды нужно для обеих проверок обнаружения сигнала и энергии во время процесса оценки чистого канала [CCA]. Думайте об обнаружении сигнала как о методе обнаружения и задержки радио передачи 802.11. Думайте об обнаружении энергии как о методе обнаружения и задержки любого сигнала от не-802.11 передатчиков. Как показано в Таблице 8.1, оба порога используются вместе во время процесса проверки чистого канала (CCA), чтобы определить занята ли среда и соответственно отложить передачу.

**ТАБЛИЦА 8.1** Пороги проверки чистого канала

Обнаружение Сигнала Signal Detect (SD)	Обнаружение Энергии Energy Detect (ED)	Передать или Задержать
Пусто (Idle)	Пусто (Idle)	Можно передавать
Занято (Busy)	Пусто (Idle)	Задержать и начать демодулировать символ OFDM
Пусто (Idle)	Занято (Busy)	Задержать на один временной слот OFDM

В стандарте 802.11-2020 определения обоих этих порогов CCA отчасти нечёткие, что часто приводят к неправильному пониманию реальных значений порогов. Трактовка этих порогов Wi-Fi производителями радиомодулей для клиентов 802.11 и ТД часто отличаются. Чтобы усложнить дело еще больше, вспомните, пожалуйста, что возможности приемной чувствительности между радиомодулями могут широко варьироваться. Из-за различия в приемной чувствительности, восприятие уровня шума может быть совершенно разным между радиомодулями 802.11. Следовательно, два порога оценки чистого канала CCA могут также варьироваться из-за разниц в приемной чувствительности. Пороги CCA, обсуждаемые в этом разделе, основаны на передачах на 20 МГц каналах. В Главе 10 «Технология MIMO: НТ и VHT» вы узнаете, что радиомодули 802.11n, 802.11ac, 802.11ax имеют возможность передавать на более широких каналах, объединяя вместе несколько 20МГц каналов. Например, радиомодуль 802.11n/ac/ax может передавать и принимать 40МГц канал, используя объединенные первичный и вторичный каналы. Пожалуйста, осознайте, что пороги CCA между первичным и вторичным каналами также отличаются, это будет обсуждаться позже в этой главе.

## Виртуальный Контроль Несущей

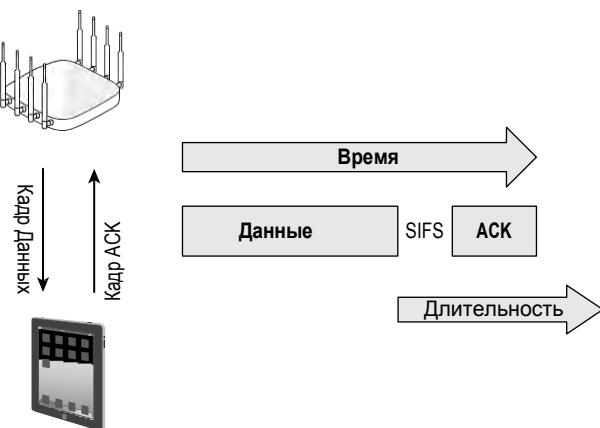
Как показано на Рисунке 8.3, одно из полей в заголовке MAC кадра 802.11 - это поле *Duration/ID* [Продолжительность/ID]. Когда клиент передает односторонний [unicast] кадр, поле Duration/ID содержит значение от 0 до 32767.

Значение Duration/ID представляет время, в микросекундах, которое требуется для передачи для активного процесса обмена кадрами для того, чтобы другие радиомодули не прерывали процесс. В примере, показанном на Рисунке 8.4, клиент, который передает кадр данных, вычислил сколько времени займет, чтобы получить кадр ACK, и включил это значение времени в поле длительности - Duration/ID в заголовке MAC переданного одностороннего кадра данных. Значение поля Duration/ID в заголовке следующего MAC кадра равно 0 (ноль). Кадр, который несет значение длительности никогда не перекрывается значением внутри кадра. Вместо этого, значение длительности в любом кадре всегда примерное количество времени, необходимое, чтобы завершить оставшийся обмен кадрами между двумя радиомодулями. Например, значение длительности кадра данных в Рисунках 8.3 и 8.4 является показателем количества времени, необходимого, чтобы ответить на односторонний обмен кадром подтверждения ACK. Подводя итог, значение поля Duration/ID показывает как долго радиосреда будет занята во время обмена кадрами, прежде чем другая станция может побороться за среду.

**Р И С У Н О К 8 . 3** Поля Duration/ID

```
IEEE 802.11 QoS Data, Flags: .p.....TC
Type/Subtype: QoS Data (0x0028)
Frame Control Field: 0x8841
    .000 0000 0010 1100 = Duration: 44 microseconds
Receiver address: Aerohive_76:b5:68 (08:ea:44:76:b5:68)
Transmitter address: Apple_0f:dd:f4 (7c:fa:df:0f:dd:f4)
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
Source address: Apple_0f:dd:f4 (7c:fa:df:0f:dd:f4)
BSS Id: Aerohive_76:b5:68 (08:ea:44:76:b5:68)
STA address: Apple_0f:dd:f4 (7c:fa:df:0f:dd:f4)
.... .... .... 0000 = Fragment number: 0
0000 0000 1101 .... = Sequence number: 13
Frame check sequence: 0x64aaef3c0 [correct]
FCS Status: Good!
```

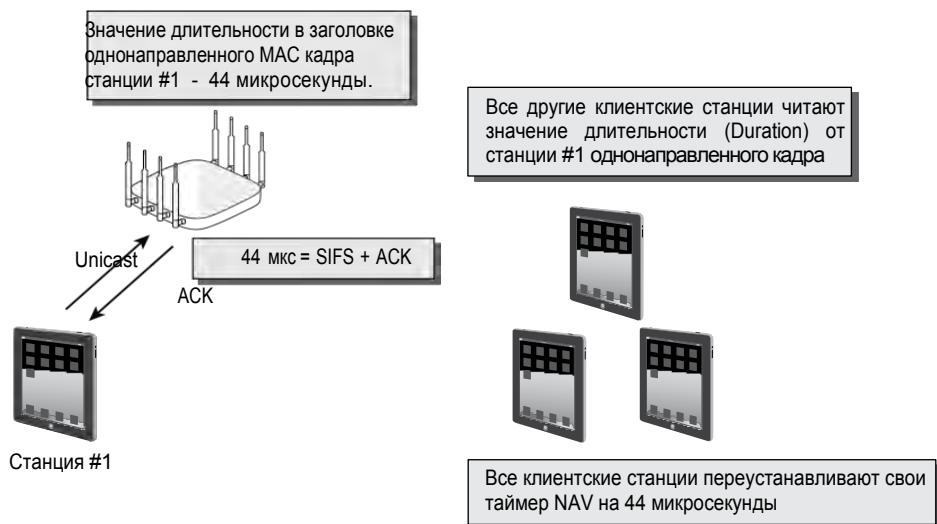
**Р И С У Н О К 8 . 4** Значение длительности SIFS + ACK



Большую часть времени поле Duration/ID содержит значение Duration (длительности), которое используется чтобы переустановить (reset) таймеры вектора занятости сети (network allocation vector (NAV)) других станций. В редких случаях кадра PS-Poll, Duration/ID используется в качестве значения ID (идентификатора) клиентской станции, используя устаревшее управление мощностью/энергией (power management). Управление мощностью/энергией обсуждается в Главе 9 «802.11 MAC»

*Виртуальный контроль несущей [Virtual carrier sense]* использует временной механизм, который называется *вектором распределения сети [network allocation vector (NAV)]*. Таймер NAV управляет предсказанием будущего трафика в среде на основе информации значения длительности (Duration) полученной в предыдущем кадре передачи. Когда радиомодуль 802.11 не передает, он слушает. Как изображено на Рисунке 8.5, когда слушающий радиомодуль слышит передачу кадра от другой станции, он смотрит в заголовок кадра и определяет содержит ли поле Duration/ID значение длительности (Duration) или значение идентификатора (ID). Если поле содержит значение Длительности (Duration), слушающая станция установит свой таймер NAV в это значение. Слушающая станция затем будет использовать NAV в качестве таймера обратного отсчета, зная, что радиосреда будет занята пока отсчет не достигнет 0.

**Р И С У Н О К 8 . 5** Виртуальный контроль несущей



Этот процесс по существу позволяет передающему радиомодулю 802.11 уведомить другие станции, что среда будет занята на период времени (значения Duration/ID). Станции, которые не осуществляют передачу, слушают и слышат Duration/ID, устанавливают таймер обратного отсчета (NAV), и ждут пока их таймер достигнет 0, прежде чем они могут побороться за среду и, в итоге, осуществить передачу по среде.

Станция не может бороться за среду до тех пор ее таймер NAV не достигнет 0, не может станция вести передачу по радиосреде, если таймер NAV установлен в ненулевое значение. Как ранее утверждалось, CSMA/CA использует несколько линий обороны, чтобы предотвратить конфликты, и таймер NAV часто рассматривается как одна линия обороны.

Так как значение Duration/ID в заголовке MAC 802.11 используется для установки таймера NAV, то виртуальный контроль несущей является механизмом контроля несущей на 2 уровне.

Важно понять, что и виртуальный контроль несущей и физический контроль несущей всегда происходят одновременно. Виртуальный контроль несущей – это линия обороны 2 уровня, в то время как физический контроль несущей – линия обороны 1 ого уровня. Если одна линия обороны провалилась, есть надежда, что другая предотвратит от того, что произойдут конфликты (коллизии).

## Псевдо Случайный Таймер Отсрочки

Станции 802.11 могут бороться за среду в течении окна времени, называемого *временем отсрочки [backoff time]*. В этой точке в процессе CSMA/CA, станция выбирает случайное значение отсрочки, используя псевдо-случайный алгоритм отсрочки.

Станция выбирает случайное число из диапазона, называемое значение *окна конкурентной борьбы [contention window (CW)]*. После того как случайное число выбрано, число умножается на величину времени временного интервала или временного слота [*slot time*]. Это запускает таймер псевдо-случайной отсрочки. Пожалуйста, не перепутайте таймер отсрочки с таймером NAV. Как упоминалось ранее, таймер NAV – это механизм виртуального контроля несущей, используемого, чтобы зарезервировать среду для дальнейшей передачи. Псевдослучайный таймер отсрочки – это финальный таймер, используемый станцией перед ее передачей. Таймер отсрочки станции начинает обратный отсчет тактов, называемых интервалами или слотами [*slots*]. Когда таймер отсрочки равен нулю, клиент может заново оценивать канал, и, если он чист, начать передачу.

Размеры временных слотов зависят от используемой спецификации Физического уровня (PHY). Например, устаревшие радиомодули 802.11b используют HR-DSSS PHY, который определяет слот времени в 20 мкс (μs). Все радиомодули 802.11 a/g/n/ac используют мультиплексирование с ортогональным частотным разделением (OFDM) и слотом времени в 9 мкс(μs). В течении слота времени OFDM, 4 мкс(μs) нужны для обнаружения сигнала (SD) и обнаружение энергии (ED) контроля несущей, и 4 мкс(μs) нужны для прослушивания OFDM символа.

Если никакой активности в среде не произошло в течении определенного интервала времени (временного слота), то таймер отсрочки уменьшается на интервал времени (на один тайм слот). Если механизмы физического или виртуального контроля несущей обнаружили, что среда занята, то уменьшение таймера отсрочки останавливается, а значение таймера отсрочки сохраняется. Когда среда является пустой в течении длительности DIFS, AIFS или EIFS период, процесс отсрочки возобновляется и продолжается обратный отсчет с того места, где остановился. Когда таймер отсрочки достигает нуля, начинается передача. Следующий пример – простой обзор всего процесса отсрочки:

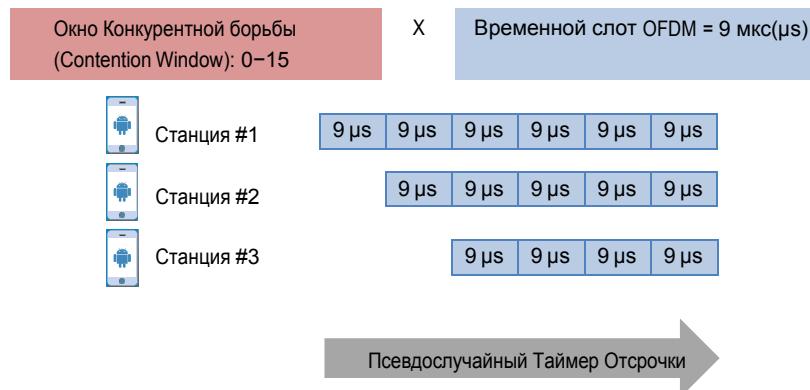
- Станция OFDM выбирает случайное число из окна конкурентной борьбы от 0 до 15. Для этого примера выбралось 4.
- Станция умножает случайное число на временной интервал (тайм слот) 9мкс(μs).
- Случайный таймер отсрочки имеет значение 36мкс (4 слота).
- Для каждого интервала(слота) времени, в течении которого нет активности в среде, таймер отсрочки уменьшается на один слот (интервал) времени.
- Станция уменьшает таймер отсрочки пока таймер не станет равным нулю.
- Станция выполняет финальную оценку чистого канала (CCA) и передает, если среда чистая.
- Если среда не чистая, то клиент задерживается на один интервал времени, оценивает среду с другой проверкой CCA , и затем передает, если среда чистая.

Весь смысл процедуры отсрочки [backoff] в том, что радиомодули 802.11 получают шанс на передачу в радиосреде; однако псевдослучайный процесс необходим, чтобы гарантировать, что все они получат свое время. Хорошой аналогией будет пример: записать числа от 0 до 15 на 16 кусочках бумаги и положить все кусочки в шляпу. Затем четыре человека будут

выбирать по одному кусочку бумаги из шляпы. Человек с наименьшим номером будет передавать в эфир первым.

Рисунок 8.6 иллюстрирует процесс по-другому. Предположим, что три клиента 802.11ac на канале 40 хотят передать в одно и тоже время. Длина таймера отсрочки каждой станции абсолютно случайны и базируются на окне конкурентной борьбы. Клиентской станции #1 может быть присвоено значение CW = 6, умноженное на 9 мкс ( $\mu$ s) интервала времени, получаем таймер отсрочки 54 мкс ( $\mu$ s). Клиентской станции #2 может быть присвоено значение CW=5, умноженное на 9 мкс слота времени, получаем таймер отсрочки 45 мкс ( $\mu$ s). Клиентской станции #3 может быть присвоено значение CW = 4, умноженное на 9 мкс ( $\mu$ s), получаем таймер отсрочки равный 36 мкс ( $\mu$ s). Все три станции затем начинают уменьшать свои таймеры отсрочки по 9 мкс( $\mu$ s) слота времени. Таймер отсрочки станции #3 уменьшится первым, и она первая будет передавать в эфир.

**РИСУНОК 8.6** Псевдослучайный таймер отсрочки



Вспоминаем, что радиосреда является полудуплексной, и что только один радиомодуль может передавать одновременно. Следовательно, все радиомодули 802.11 должны бороться за эфир, включая радиомодули любой точки доступа. Внутри любого базового состава сервиса (BSS), ТД всегда являются наиболее загруженным передатчиком; однако, радиомодулю ТД не дано никакого специального приоритета, и он должен также бороться за эфир вместе со всеми клиентами, которые могут быть ассоциированы с этой ТД.

Случайный таймер отсрочки является еще одной линией обороны и помогает минимизировать вероятность двух станций попытаться выйти в эфир в одно и то же время, хотя это не полностью предотвращается. Если станция не получает ACK, она запускает процесс контроля несущей заново. Что, если передача кадра повреждена и требуется повторная передача? Неудачные передачи приводят к тому, что размер CW увеличивается экспоненциально до максимального значения, как показано на Рисунке 8.7. Другими словами, станции должны бороться за эфир для любой повторной передачи; однако, шансы не обязательно будут такими же хорошими с каждой последующей повторной передачей. Это гарантирует лучшую стабильность при условиях высокой емкости.

**РИСУНОК 8.7**  
(CW)

Пример экспоненциального увеличения окна конкурентной борьбы



## Межкадровое Пространство

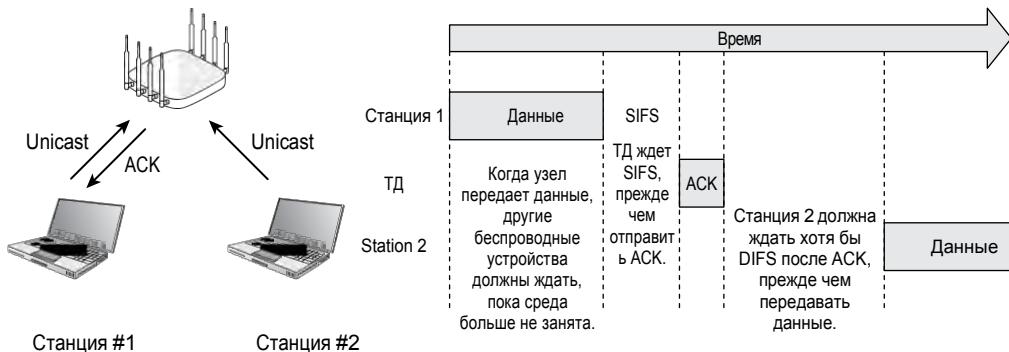
*Межкадровое пространство [Interframe space (IFS)]* - это период времени, который существует между передачами беспроводных кадров. Существует 10 типов межкадровых пространств. Далее дан частичный список, от кратчайшего до самого длинного:

- Уменьшенное межкадровое пространство (RIFS) — наивысший приоритет
- Короткое межкадровое пространство (SIFS) — второй наивысший приоритет
- Приоритетное межкадровое пространство (PIFS) — средний приоритет
- DCF межкадровое пространство (DIFS) — низший приоритет
- Арбитражное межкадровое пространство — используется станциями с поддержкой качества (QoS)
- Расширенное межкадровое пространство (EIFS) — используется после получения поврежденных кадров

Реальная длительность каждого межкадрового пространства варьируется в зависимости от скорости передачи сети. Межкадровые пространства являются еще одной линией обороны, используемой CSMA/CA, чтобы гарантировать, что только определенные типы кадров 802.11 передаются следуя за определенным межкадровыми пространствами. Например, только кадры ACK, блок кадров ACK, кадры данных, и кадры разрешения на отправку [clear-to-send (CTS)] могут следовать за SIFS. Два наиболее часто используемых межкадровых пространства - это SIFS и DIFS. Как нарисовано на Рисунке 8.8, кадр ACK - это кадр с наивысшим приоритетом, и использование SIFS гарантирует, что он будет передан первым, перед любым другим типом кадра 802.11.

Большинство других кадров 802.11 следуют за более длительным периодом, называемом DIFS. Станции используют SIFS, чтобы поддерживать управление средой во время последовательности обмена кадров. Другие станции не могут получить доступ к среде во время этой последовательности, потому что они должны ждать более долгий DIFS.

**РИСУНОК 8.8** SIFS и DIFS



Все межкадровые пространства определяют какой тип трафика 802.11 разрешен следующим. Межкадровое пространство также действует как резервный механизм для виртуального контроля несущей, который обсуждался ранее в этой главе.

## Функция Гибридной Координации

Поправка о качестве сервиса (QoS) 802.11e добавила новую координационную функцию для конкурентной борьбы за среду 802.11, которая называется, как *Функция Гибридной Координации [Hybrid Coordination Function (HCF)]*. Поправка 802.11e и HCF с тех пор включены в стандарт 802.11-2020. HCF использует существующие возможности DCF (функции распределенной координации) и добавляет улучшения, чтобы создать два способа по доступу к каналу: Расширенный Распределенный Доступ к Каналу [Enhanced Distributed Channel Access (EDCA)] и Доступ к Каналу, Контролируемый Функцией Гибридной Координации [HCF Controlled Channel Access (HCCA)].

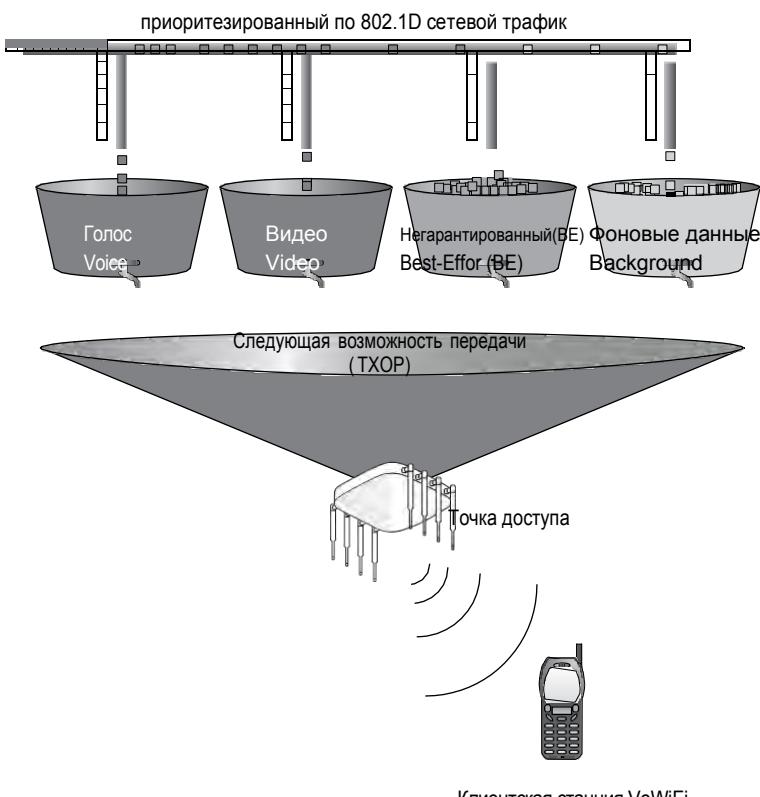
Механизмы борьбы за среду функции распределенной координации (DCF), обсужденные ранее, позволяют радиомодулю 802.11 передавать один кадр. После передачи кадра, станция 802.11 должна бороться за среду снова, прежде чем передать следующий кадр. HCF определяет возможность радиомодулю 802.11 отправить несколько кадров за время передачи по радиосреде. Когда радиомодуль, совместимый с HCF, борется за среду, он получает выделенное количество времени, чтобы передать кадры. Этот период времени называется *возможностью передачи [transmit opportunity (TXOP)]*. Во время этого TXOP радиомодуль 802.11 может отсыпал один или несколько кадров. Во время TXOP несколько кадров могут быть отправлены последовательно, в так называемой *взрывной серии кадров [frame burst]*. Короткое межкадровое пространство [*short interframe space (SIFS)*] используется между каждым кадром, чтобы гарантировать, что никакой другой радиомодуль не передает во время взрывной серии кадров. Однако, агрегация кадров является более обычным методом по отправке нескольких кадров во время TXOP. *Агрегация кадров [Frame aggregation]* - это метод объединения нескольких кадров в один кадр передачи во время TXOP. Два способа агрегации кадров будут описаны в Главе 10.

## Расширенный Распределенный Доступ к Каналу

*Расширенный Распределенный Доступ к Каналу [Enhanced Distributed Channel Access (EDCA)]* - это метод доступа к беспроводной среде, который обеспечивает дифференцированный доступ, который направляет трафик по четырем очередям с приоритетом качества сервиса (QoS) категории доступа. EDCA это расширение DCF (распределенной координационной функции). Способ доступа к среде EDCA распределяет по приоритетам (приоритезирует) трафик, используя метки приоритета, которые идентичны меткам (tag) приоритета 802.1D. Метки приоритета обеспечивают механизм применения качества сервиса (QoS) на уровне MAC.

Доступны различные классы сервиса, представленные в 3х битном поле пользовательского приоритета [user priority (UP)] в заголовке IEEE 802.1Q, добавленном к кадру Ethernet. 802.1D включает очередьизацию по приоритетам (позволяя некоторым кадрам Ethernet пересыпаться раньше других в коммутируемой Ethernet сети). Рисунок 8.9 изображает метки приоритета 802.1D со стороны Ethernet, которые используются для распределения трафика по очередям каждой категории доступа.

**РИСУНОК 8.9**      Метки приоритета EDCA и 802.1D



EDCA определяет четыре категории доступа, базирующихся на восьми пользовательских приоритетах (UP). Четыре категории доступа, от низшего приоритета до высшего приоритета, это - Фоновые данные (AC\_BK (Background)), Обычные данные с негарантированной доставкой (AC\_BE (Best Effort)), Видео (AC\_VI (Video)), и Голос (AC\_VO (Voice)). Для каждой категории доступа, используется расширенная версия DCF,

называемая *Функцией Расширенного Распределенного Доступа к Каналу [Enhanced Distributed Channel Access Function (EDCAF)]*, чтобы бороться за TXOP. Кадры с категорией доступа с наивысшим приоритетом имеет наименьшее значение, и следовательно наиболее вероятно получит TXOP. Детальные характеристики этого процесса находятся за пределами экзамена CWNA.

## Доступ к Каналу, Контролируемый Функцией Гибридной Координации (HCCA)

*Доступ к Каналу, Контролируемый Функцией Гибридной Координации [HCF Controlled Channel Access (HCCA)]* является optionalным методом доступа к беспроводной среде, который использует централизованный координатор с поддержкой качества сервиса (QoS), который называется *гибридный координатор [hybrid coordinator (HC)]*. Гибридный Координатор [HC] встроен в точку доступа и имеет более высокий приоритет доступа к беспроводной среде. Используя этот более высокий уровень приоритета, он может занять TXOP для себя и других станций, чтобы обеспечить ограниченную по времени фазу контролируемого доступа [controlled access phase (CAP)], обеспечивающую свободную от конкурентной борьбы передачу данных с поддержкой качества сервиса(QoS). Детальные характеристики этого процесса находятся за пределами экзамена CWNA. На момент написания, мы не знали ни одного производителя, который бы внедрил HCCA.

## Wi-Fi Мультимедиа

До принятия поправки 802.11e, не было ни какого адекватного определения процедуры качества сервисов (QoS) для использования чувствительных ко времени приложений, например *Голос поверх Wi-Fi [Voice over Wi-Fi (VoWiFi)]*. Трафик приложения, такого как голос, звук и видео имеет низкий допуск к задержке и джиттеру (вариации задержки), и требует приоритет перед стандартным трафиком данных. Поправка 802.11e определяет методы второго, MAC уровня, необходимых, чтобы удовлетворить требованиям качества (QoS) для чувствительных ко времени приложений в беспроводном ЛВС 802.11. Wi-Fi Альянс представил сертификацию *Wi-Fi Мультимедиа [Wi-Fi Multimedia (WMM)]*, как частичное отражение поправки 802.11e.

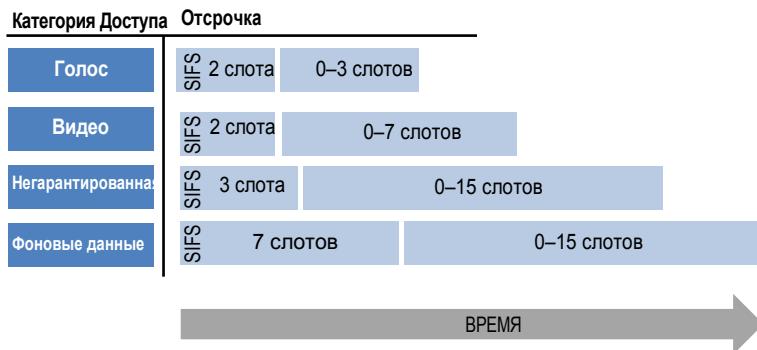
Так как WMM основан на механизмах EDCA, метки приоритета 802.1D со стороны Ethernet используются, чтобы направлять трафик по четырем очередям с приоритетом категории доступа. Сертификация WMM предоставляет приоритезацию трафика по четырем категориям доступа, описанным в Таблице 8.2.

**ТАБЛИЦА 8.2** Категории доступа Wi-Fi мультимедиа

Категория доступа	Описание	Метки 802.1D
WMM Voice priority Приоритет для голоса	Это высший приоритет. Он позволяет осуществлять несколько одновременных VoIP звонков с низкой задержкой и качеством платных звонков.	7, 6
WMM Video priority Приоритет для Видео	Этот приоритет поддерживает приоритезированный видео трафик перед другим трафиком передачи данных. Один канал 802.11g или 802.11a может поддерживать три-четыре SDTV видеопотока или один HDTV видеопоток.	5, 4
WMM Best Effort priority Приоритет для Негарантированного трафика	Это трафик от приложений и устройств, таких как просмотр Интернета, который не может предоставить возможности QoS, таких как устаревшие устройства. Этот трафик не чувствителен к задержке, но подвержен негативному влиянию длительных задержек.	0, 3
WMM Background priority Приоритет для фоновых данных	Это низкоприоритетный трафик, который не имеет строгих требований к полосе или задержкам. Этот трафик включает передачу файлов и отправку на печать.	2, 1

Весь смысл WMM - приоритезировать разные классы трафика приложений во время процесса борьбы за среду. Как показано на Рисунке 8.10, категория доступа для голоса имеет лучшие шансы при борьбе за среду во время процесса отсрочки [backoff]. Для голосового трафика требуемое время ожидания минимум: SIFS плюс два временных интервала (слота) и еще окно конкурентной борьбы от 0 до 3х слотов, прежде чем передавать в эфир. Негарантированный [Best-effort] трафик должен ждать минимум SIFS и три слота, а затем окно конкурентной борьбы от 0 до 15 слотов. Процесс борьбы все еще псевдо случайный; однако, шансы лучше для голосового трафика.

**Р И С У Н О К 8.10** Распределение времени по категориям доступа WMM



Wi-Fi Альянс также определил *-WMM-PS* [*Power Save* (*Сбережение Энергии*)], которое использует механизмы экономии энергии 802.11e, чтобы увеличить срок жизни батареи клиентских устройств. Вы можете найти больше информации о управлении энергией в Главе 9.

Еще одна сертификация Wi-Fi Альянса – это *WMM-Контроль Допуска* [*WM M-Admission Control*], которая определяет использование кадров управления для сигнализации между ТД и клиентской станцией. Станция-клиент может запросить отправку потока трафика [*traffic stream (TS)*] кадров определенной категории доступа WMM. Поток трафика может быть односторонним или двунаправленным. ТД оценивает кадр запроса относительно загрузки сети и состояния канала. Если ТД может удовлетворить запрос, она принимает запрос и дает клиентской станции время в эфире для потока трафика. Если запрос отклонен, то клиентскому устройству не разрешено начинать запрошенный поток трафика, и он может решить задержать поток трафика, ассоциироваться с другой ТД, или установить поток best-effort трафика за пределами работы WMM-Контроля Допуска. WMM-Контроль Допуска [*WMM-Admission Control*] улучшает производительность чувствительных ко времени данных, таких как видео и голос. WMM-Контроль Допуска [*WMM-Admission Control*] также улучшает надежность приложений во время работы путем предотвращения переиспользования (переподписки - *oversubscription*) полосы

**Важные Информационные Бюллетени (Белые Листы) Wi-Fi Альянса**

У Wi-Fi Альянса есть два белых листа, которые мы рекомендуем вам прочитать, чтобы узнать больше о WMM. Оба белых листа доступны для скачивания на сайте Wi-Fi Альянса: [www.wi-fi.org](http://www.wi-fi.org).

- *Wi-Fi CERTIFIED for WMM (СЕРТИФИЦИРОВАННЫЙ Wi-Fi для WMM)*
- *Wi-Fi CERTIFIED for WMM Power Save (СЕРТИФИЦИРОВАННЫЙ Wi-Fi для Сбережения Энергии WMM)*

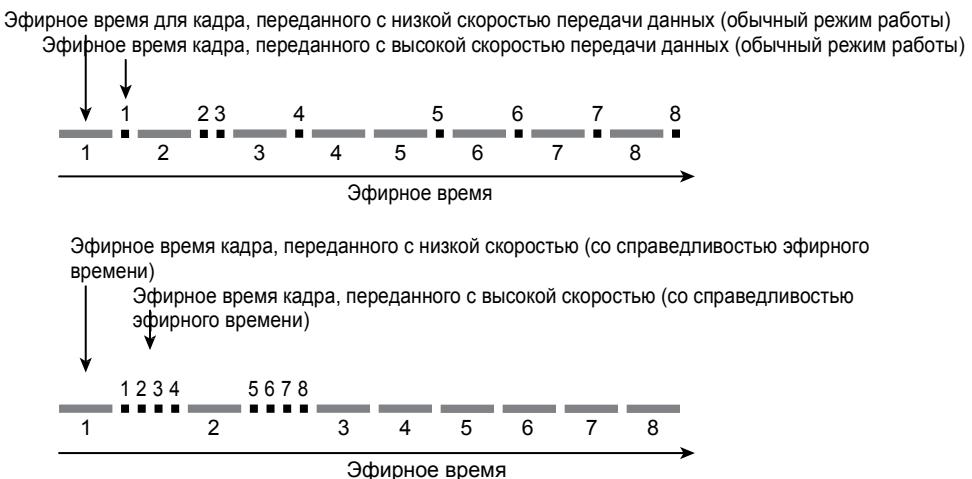
## Справедливость Эфирного Времени (Airtime Fairness)

Одна из важных характеристик 802.11 это его способность поддерживать много различных скоростей передачи данных. Это позволяет старым технологиям продолжать поддерживать связь параллельно более новым устройствам, вместе с возможностью устройствам поддерживать связь, переключая на пониженную скорость передачи данных, по мере того, как они отдаляются от точки доступа. Способность использовать эти более низкие скорости передачи данных является первостепенной важности для связи 802.11; однако, она может также быть огромным препятствием для общей производительности сети и отдельных устройств, работающих на более высоких скоростях передачи данных.

Так как 802.11 основан на борьбе, каждый радиомодуль должен бороться за свое время связи, затем осуществить трансляцию, и затем снова вернуться к процессу борьбы. Когда каждый радиомодуль получает свое время передачи, другие радиомодули 802.11 должны ждать. Если передающий радиомодуль использует высокие скорости передачи данных, другие радиомодули не должны долго ждать. Если передающий радиомодуль использует низкие скорости передачи данных, другие радиомодули должны ждать намного больший период времени. Когда радиомодули 802.11 передают на очень низкой скорости, такой как 1Мбит/с и 2Мбит/с, фактически они являются причиной накладных расходов [overhead] борьбы за среду для более высокоскоростных передатчиков из-за длительного времени ожидания, пока медленные устройства осуществляют передачу.

Чтобы попытаться понять это, взгляните на Рисунок 8.3. Верхняя часть рисунка иллюстрирует нормальную работу двух станций, каждая посыпает восемь кадров. Одна станция посыпает восемь кадров на более высоких скоростях передачи данных, а другая станция посыпает восемь кадров с более низкой скоростью передачи данных. Если высокоскоростное и низкоскоростное устройства существуют в одной и той же БЛВС, они должны делить или бороться за время передачи. Другими словами, обе станции статистически получат одинаковое количество раз доступ к радиосреде, несмотря на то, что одна из станций способна передавать на большей скорости передачи данных и требует намного меньше эфирного времени, чтобы передать такое же количество данных. Так как никакого приоритета не задано для станции с более высокой скоростью передачи данных, обе станции закончат передавать свои восемь кадров за один и тот же период времени.

**РИСУНОК 8.11** Пример справедливости эфирного времени



Вместо назначения равного доступа к сети между устройствами, цель *справедливости эфирного времени* [*airtime fairness*] назначить равное время, а не равные возможности. Справедливость эфирного времени может обеспечить лучшее управление временем радиосреды. В нижней половине Рисунка 8.11, включена справедливость эфирного времени; вы можете увидеть, что станции с большей скоростью передачи данных дан приоритет по передаче перед станцией с низкой скоростью передачи данных. Фактически, это намного лучшее использование времени передачи, потому что станции с высокой скоростью передачи данных не нужно сохранять молчаливое ожидание во время низкоскоростной передачи данных. Заметьте, что быстрая станция передает все восемь кадров за много меньший период времени, а станция с низкой скоростью передачи данных также посыпает все восемь кадров примерно за тот же период, что и прежде. Справедливость эфирного времени эффективно обеспечивает лучшее управление временем среды за счет сокращения времени ожидания. Чистый результат – лучшая производительность, большая емкость, и больше пропускной способности по сети Wi-Fi.

На текущий момент, никакой стандарт или поправка 802.11 не определяют справедливость эфирного времени или как внедрить её, ни от какого производителя не требуется внедрять это. Большинство производителей используют механизмы справедливости времени только для нисходящей [*downstream*] передачи от точки доступа к ассоциированным клиентам. Механизмы справедливости эфирного времени обычно используются для приоритезации высокоскоростных нисходящих (*downstream*) передач данных от ТД над низкоскоростными нисходящими передачами данных от ТД. По крайней мере один производитель также заявил о поддержке справедливости эфирного времени в восходящем (*upstream*) потоке. Любая реализация справедливости эфирного времени является собственным решением, разработанным каждым производителем БЛВС самостоятельно. Не важно как каждый производитель реализует это решение, основная цель, по существу, одна и та же: помешать низкоскоростным устройствам замедлить оставшуюся сеть.

Хотя каждый производитель БЛВС использует свой подход к реализации

справедливости эфирного времени, типовым для них является анализ нисходящего клиентского трафика и присвоение различных весов, основанных на таких параметрах как текущая пропускная способность, клиентская скорость передачи данных, SSID, тип PHY, и другие переменные. Далее используются алгоритмы для обработки этой информации и определения числа возможностей для каждой клиентской нисходящей передачи. Если все применено правильно, то справедливость эфирного времени улучшает использование среды путем предоставления преимущественного доступа для высокоскоростных передач данных..

## Итого

Эта глава сосредоточена на доступе к среде 802.11. Каждая станция имеет право на связь, и управление доступом к беспроводной среде контролируется посредство контроля доступа к среде [MAC]. Мы обсудили разницу между CSMA/CD и CSMA/CA как методов конкурентной борьбы. CSMA/CA использует псевдо случайный метод борьбы, называемый Функцией Распределенной Координации [Distributed Coordination Function (DCF)]. DCF использует четыре линии защиты, чтобы гарантировать, что только один радиомодуль 802.11 передает в полудуплексную среду.

Поправка о качестве сервиса 802.11e добавила новую координационную функцию к борьбе за среду 802.11, называемую Гибридная Координационная Функция (Hybrid Coordination Function (HCF)). Сертификация Wi-Fi Мультимедиа (WMM) была представлена Wi-Fi Альянсом как частичное отражение поправки 802.11e. WMM создана, чтобы удовлетворить требования качества сервисов (QoS) для чувствительных ко времени приложений, таких как звук, видео и голос поверх IEEE 802.11.

Справедливость Эфирного времени [Airtime fairness] была представлена, как метод для производителей для обеспечения более быстрым устройствам преимущественный доступ к среде при параллельной работе с устройствами, которые передают на более низких скоростях передачи данных.

## Темы Экзамена

**Понимать схожести и отличия между CSMA/CA и CSMA/CD.** Понимать оба метода доступа и знать, что делает их похожими и что делает их различными.

**Дать определение четырем мерам и весам CSMA/CA и DCF.** Понимать, что виртуальный контроль несущей, физический контроль несущей, межкадровое пространство, и псевдо-случайный таймер отсрочки работают все вместе, чтобы гарантировать, что только один радиомодуль 802.11 передает в полудуплексную среду.

**Дать определение виртуальному контролю несущей и физическому контролю несущей.** Понимать назначение и базовые механизмы двух способов контроля несущей.

**Дать определение механизмам качества сервиса HCF.** Функция Гибридной Координации определяет использование TXOP и категорий доступа в EDCA, также как использование TXOP и опроса во время HCCA.

**Понимать сертификацию Wi-Fi мультимедиа.** WMM разработана, чтобы обеспечить возможности качества-сервиса в беспроводных сетях 802.11. WMM является частичным отражением поправки 802.11e. На текущий момент WMM предоставляет приоритет трафику по четырем категориям доступа.

**Понимать важность справедливости эфирного времени [airtime fairness] и что она делает.** Справедливость эфирного времени предоставляет устройствам, работающим на более быстрых скоростях, преимущественный доступ к среде. Этот преимущественный режим обеспечивает всем устройствам равный доступ, в результате чего все устройства в равной степени используют доступную полосу пропускания для передачи.

# Контрольные Вопросы

1. Какой метод доступа и борьбы за среду используется в качестве основы Функции Распределенной Координации (DCF) 802.11?
  - A. Множественный Доступ с Контролем Несущей и Обнаружением Конфликтов [Carrier Sense Multiple Access with Collision Detection (CSMA/CD)]
  - B. Множественный Доступ с Контролем Несущей и Предотвращением Конфликтов [Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)]
  - C. Передача жетона(токена) [Token passing]
  - D. Запрос приоритета [Demand priority]
2. Обнаружение конфликтов 802.11 достигается с использованием какой технологии?
  - A. Вектор распределения сети [Network allocation vector (NAV)]
  - B. Проверка чистоты канала [Clear channel assessment (CCA)]
  - C. Значение Duration/ID
  - D. Получение подтверждения (ACK) от станции назначения
  - E. Положительное обнаружение конфликта(коллизии) не может быть определено.
3. Кадры ACK и CTS следуют за каким межкадровым пространством?
  - A. EIFS
  - B. DIFS
  - C. PIFS
  - D. SIFS
  - E. AIFS
4. Часть контроля несущей CSMA/CA выполняется используя какой из следующих методов? (Выберите все, что применимо.)
  - A. Окно конкурентной борьбы [Contention window]
  - B. Таймер отсрочки [Backoff timer]
  - C. Окно контроля канала [Channel sense window]
  - D. Проверка чистоты канала [Clear channel assessment]
  - E. Таймер NAV
5. После выполнения станцией контроля несущей и обнаружения, что никакое другое устройство не передает за период интервала DIFS, какой следующий шаг станции?
  - A. Ждать необходимое число слотов времени до передачи, если значение отсрочки уже было выбрано.
  - B. Начать передачу.
  - C. Выбрать значение случайной отсрочки.
  - D. Запустить таймер случайной отсрочки

6. Физический контроль несущей использует какие пороги во время оценки чистоты канала, чтобы определить занята ли среда?
- A. Обнаружение радио [RF detect]
  - B. Обнаружения сигнала [Signal detect]
  - C. Обнаружение передачи [Transmission detect]
  - D. Обнаружение энергии [Energy detect]
  - E. Случайное обнаружение [Random detect]
7. Какие из следующих терминов связаны с механизмом виртуального контроля несущей? (Выберите все, что применимо.)
- A. Окно конкурентной борьбы [Contention window]
  - B. Вектор распределения сети [Network allocation vector]
  - C. Таймер случайной отсрочки [Random backoff time]
  - D. Поле Длительность/ID [Duration/ID field]
8. Цель выделения равного времени против равной возможности называется как что?
- A. Справедливость доступа [Access fairness]
  - B. Гибкий доступ к среде [Opportunistic medium access]
  - C. CSMA/CA
  - D. Справедливость эфирного времени [Airtime fairness]
9. CSMA/CA и DCF определяют какой механизм, который пытается гарантировать, что только один радиомодуль 802.11 может передавать в полудуплексную радиосреду? (Выберите все, что применимо.)
- A. Таймер псевдо-случайной отсрочки
  - B. Виртуальный контроль несущей
  - C. Обнаружение конфликта
  - D. Физический контроль несущей
  - E. Межкадровое пространство
10. Сертификация Wi-Fi Альянса, названная Wi-Fi Мультимедиа (WMM), основана на каком методе доступа к беспроводной среде, определенном стандартом 802.11-2020?
- A. DCF
  - B. EDCA
  - C. HCCA
  - D. HSRP
11. Функция Гибридной Координации (HCF) определяет какой выделенный период времени, в котором станция может передать несколько кадров?
- A. Целевое время пробуждения [Target wake time]
  - B. Справедливость эфирного времени [Airtime fairness]
  - C. Таймер случайной отсрочки [Random backoff timer]

- D. Таймер NAV
  - E. Возможность передачи [Transmit opportunity]
12. WMM основан на EDCA и обеспечивает приоритезацию трафика через какие следующие категории доступа? (Выберите все, что применимо.)
- A. WMM Voice priority (приоритет для голоса)
  - B. WMM Video priority (приоритет для видео)
  - C. WMM Audio priority (приоритет для звука)
  - D. WMM Best Effort priority (приоритет для обычных данных)
  - E. WMM Background priority (приоритет для фоновых данных)
13. Согласно определения WMM, трафик какого типа приложения имеет наивысший приоритет для передачи в полудуплексную радиосреду?
- A. Best Effort (обычные данные)
  - B. Video (Видео)
  - C. Voice (Голос)
  - D. Background (Фоновые данные)
14. Какая информация, которая приходит из проводной сети, используется для назначения трафика по категориям доступа на точке доступа?
- A. Duration/ID
  - B. Метки приоритета 802.1D
  - C. MAC адрес назначения
  - D. MAC адрес источника
15. По каким двум причинам радиомодули 802.11 используют физический контроль несущей? (Выберите все, что применимо.)
- A. Для синхронизации входящих передач
  - B. Для синхронизации исходящих передач
  - C. Для переустановки NAV
  - D. Для запуска таймера случайной отсрочки
  - E. Для оценки радиосреды
16. Какой метод контроля несущей используется, чтобы обнаружить и декодировать передачи 802.11?
- A. Вектор Распределения Сети [Network allocation vector ]
  - B. Обнаружение сигнала [Signal detect]
  - C. Обнаружение энергии [Energy detect]
  - D. Виртуальный контроль несущей [Virtual carrier sense]

- 17.** Какое поле в MAC заголовке кадра 802.11 переустанавливает таймер NAV для всех слушающих станций 802.11?
- A.** QoS control (контроль качества сервиса)
  - B.** Frame control (контроль кадра)
  - C.** Duration/ID (длительность/ID)
  - D.** Sequence number (номер последовательности)
  - E.** Retry (Повтор)
- 18.** Метод доступа к среде EDCA обеспечивает приоритезацию трафика через приоритетные очереди, которые соответствуют восьми метками приоритета 801.D. Как называются приоритетные очереди EDCA?
- A.** Потоки трафика
  - B.** Категории доступа
  - C.** Приоритетные уровни
  - D.** Биты приоритета
  - E.** Уровни доступа
- 19.** Подтверждения (ACKs) требуются для каких нижеследующих кадров?
- A.** Unicast (Однонаправленный)
  - B.** Broadcast (Широковещательный)
  - C.** Multicast (Многонаправленный)
  - D.** Anycast
- 20.** Какие два компонента алгоритма псевдо-случайной отсрочки используется, чтобы создать таймер псевдо-случайной отсрочки?
- A.** Окно конкурентной борьбы [Contention window]
  - B.** Вектор распределения сети [Network allocation vector]
  - C.** Duration/ID
  - D.** Время слота [Slot time]

# Глава 9



# 802.11 MAC

---

**В ЭТОЙ ГЛАВЕ ВЫ УЗНАЕТЕ О СЛЕДУЮЩЕМ:**

- ✓ **Пакеты, кадры, и биты**
- ✓ **Канальный уровень**
  - Блок сервисных данных MAC (MSDU)
  - Блок данных протокола MAC (MSDP)
- ✓ **Физический уровень**
  - Блок сервисных данных PLCP
  - Блок данных протокола PLCP
- ✓ **Совместимость 802.11 и 802.3**
- ✓ **802.11 MAC заголовок**
  - Контрольное Поле Кадра
  - Поле Duration/ID (Длительность/ID)
  - Адресация MAC уровня
  - Поле Sequence Control (Контроль Последовательности)
  - Поле QoS Control (Контроль качества сервиса)
  - Поле HT Control (Контроль Высокой Пропускной способности)
- ✓ **Тело кадра 802.11**
- ✓ **Окончание 802.11**
- ✓ **Машина состояний 802.11**
- ✓ **Кадры управления**
  - Маяк (Beacon)
  - Аутентификация (Authentication)
  - Ассоциация (Association)
  - Переассоциация (Reassociation)



- Деассоциация (Disassociation)
- Деаутентификация (Deauthentication)
- Кадр действия

✓ Кадры Контроля

- Кадр подтверждения ACK
- Блоковое подтверждение
- PS-Poll
- RTS/CTS
- CTS-to-Self
- Механизмы защиты

✓ Кадры данных

- Кадры данных с поддержкой QoS и без QoS [non-QoS]
- Не несущие данные кадры

✓ Управление электропитанием

- Устаревшее управление питанием
- Энергосбережение WMM и U-APSD
- Управление питанием в MIMO
- Управление питанием в 802.11ax



Эта глава представляет все компоненты формата МАС кадра 802.11. Мы обсуждаем как информация верхних уровней инкапсулируется в формат кадра 802.11. Мы детально обсуждаем заголовок МАС 802.11 и МАС адресацию. Мы охватываем три главных типа кадров 802.11 и основные подтипы кадров 802.11. Мы обсуждаем машину состояний 802.11, которая определяет, как станции обнаруживают, присоединяются, и покидают базовый состав сервиса (BSS). Наконец, мы обсуждаем устаревшее управление электропитанием 802.11 и улучшенное управление электропитанием WMM-PS, какие методы используются для сохранения жизни батареи.

## Пакеты, Кадры и Биты

Изучая любую технологию, временами, вам нужно сделать шаг назад и сосредоточиться на основах. Если вы когда-либо управляли самолетом, вы знаете, что это важно, когда возникают трудности, перефокусироваться на приоритете номер один, основной цели – и это полет самолета. Навигация и связь вторичны при полете самолета. Когда имеешь дело с любой сложной технологией просто забыть основную цель; это также верно со связью 802.11, как и с полетом. В связи 802.11 основная цель – это передача пользовательских данных от одного вычислительного устройства до другого.

По мере обработки данных на компьютере и подготовки к передаче с одного компьютера на другой, данные стартуют с верхнего уровня модели OSI и спускаются вниз, пока не достигнут Физического уровня, где они в конце концов передаются на другие устройства. Изначально, пользователь может пожелать передать документ текстовой обработки (текстового процессора) со своего компьютера на общий диск на другом компьютере. Этот документ стартует с Прикладного уровня, спускается вниз до Физического уровня, передается на другой компьютер, а затем поднимается обратно по уровням модели OSI на Прикладной уровень на другом компьютере.

По мере путешествия данных вниз по модели OSI для того, чтобы быть переданными, каждый уровень добавляет информационный заголовок к этим данным. Это позволяет данным быть воссозданными, когда они получены другим компьютером. На Сетевом уровне, к данным, приходящим с уровняй 4-7, добавляется IP заголовок. IP *пакет[packet]* 3 уровня, или датаграмма, инкапсулирует данные с более высоких уровней. На Канальном уровне [Data-Link layer], добавляется заголовок МАС, и IP пакет инкапсулируется внутри *кадра[frame]*. Наконец, когда кадр достигает Физического уровня, заголовок PHY с дополнительной информацией добавляется к кадру.

Данные, фактически, передаются как отдельные биты на Физическом уровне. *Бит [bit]* – это двоичная цифра, принимающая значение или 0, или 1. Двоичные или бинарные цифры являются базовой единицей связи в цифровых вычислениях. *Байт [byte]* информации состоит из 8 битов. *Октет [octet]* – это другое название байта данных. Экзамен CWNA использует термины октет и байт взаимозаменяющими.

В этой главе, мы обсуждаем как информация верхнего уровня двигается вниз по модели OSI через Канальный [Data-Link] и Физический[Physical] уровни с точки зрения 802.11.

## Канальный Уровень

Канальный уровень 802.11 поделен на два подуровня. Верхняя часть – это подуровень *Управления Логической Связью IEEE 802.2 [Logical Link Control (LLC)]*, идентичный для всех сетей на основе 802, хотя он не используется всеми сетями IEEE 802. Нижняя часть Канального уровня – это подуровень *Управления Доступом к Среде [Media Access Control (MAC)]*. Стандарт 802.11 определяет работу на подуровне MAC.

### Блок Сервисных Данных MAC

Когда Сетевой уровень (3ий уровень) отправляет данные на Канальный уровень, эти данные передаются LLC и становятся, что называется *Блоком Сервисных Данных MAC [MAC service data unit (MSDU)]*. MSDU содержит данные от LLC и уровней 3-7.

Простое определение MSDU – это то, что это полезная нагрузка данных, которая включает IP пакет плюс некоторые данные LLC. Позже в этой главе, вы узнаете о трех основных типах кадров 802.11. Кадры управления и контроля 802.11 не несут информацию верхних уровней. Только кадры данных 802.11 несут полезную нагрузку MSDU в теле кадра. Стандарт 802.11-2020 гласит, что максимальный размер MSDU – 2304 байта. Максимальный размер тела кадра определяется максимальным размером MSDU (2304 октета), плюс всевозможные накладные расходы (или оверхед) от шифрования.

Принятие поправки 802.11n-2009 ввело агрегированный MSDU (A-MSDU). С A-MSDU, максимальный размер тела кадра определяется максимальным размером A-MSDU в 3839 или 7935 октетов, в зависимости от возможностей станции (STA), плюс любые накладные расходы от шифрования. Вы узнаете больше о A-MSDU в Главе 10, “Технология MIMO: НТ и VHT”.

### Блок Данных Протокола MAC

Когда подуровень LLC отправляет MSDU на подуровень MAC, информация MAC заголовка добавляется к MSDU, чтобы идентифицировать его. MSDU теперь инкапсулирован в блок протокола данных MAC [MAC protocol data unit (MPDU)]. Простое определение MPDU 802.11 – это то, что это кадр 802.11. Как показано на Рисунке 9.1, MPDU 802.11 состоит из следующих трех основных компонентов:

**Заголовок MAC** Контрольная информация кадра, информация о длительности, MAC адресация, контроль последовательности, контрольная информация качества сервиса (QoS), контрольная информация высокой пропускной способности (НТ) – всё это находится в заголовке MAC. Заголовок 802.11 MAC обсуждается более детально далее в этой главе.

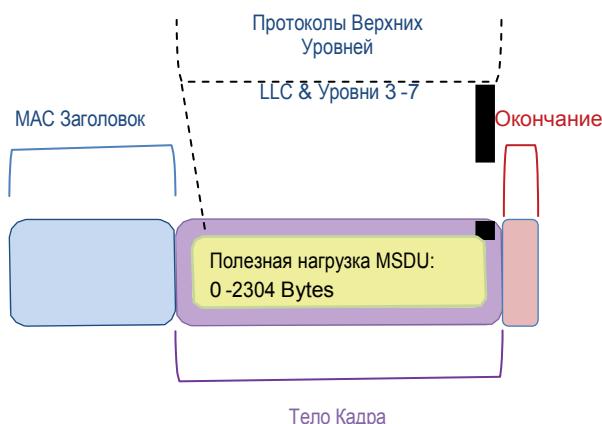
**Тело Кадра** Компонент тела кадра может варьироваться по размеру, и содержит информацию, которая различается, в зависимости от типа кадра и подтипа кадра. Полезная нагрузка верхних уровней MSDU инкапсулируется в тело кадра. Полезная нагрузка MSDU уровней 3-7 защищается с использованием шифрования.

### Последовательность Проверки Кадра [Frame Check Sequence]

Последовательность проверки кадра (FCS) содержит в себе 32 битную циклическую избыточную проверку [*cyclic-redundancy check (CRC)*], которая используется для подтверждения целостности полученных кадров.

РИСУНОК 9.1

802.11 MPDU



В этой точке, кадр готов быть переданным на Физический уровень, который затем далее подготовит кадр к передаче.

## Физический Уровень

Аналогично тому, как Канальный уровень делится на два подуровня, *Физический уровень* [*Physical layer*] также делится на два подуровня. Верхняя часть Физического уровня называется как подуровень *Процедуры Сходимости Физического Уровня* [*Physical Layer Convergence Procedure (PLCP)*], а нижняя часть называется подуровень *Зависимый от Физической Среды* [*Physical Medium Dependent (PMD)*]. PLCP подготавливает кадр к передаче, принимая кадр от MAC подуровня и создавая блок данных протокола PLCP [*PLCP protocol data unit (PPDU)*]. Подуровень PMD затем модулирует и передает данные в виде битов.

### Блок Сервисных Данных PLCP

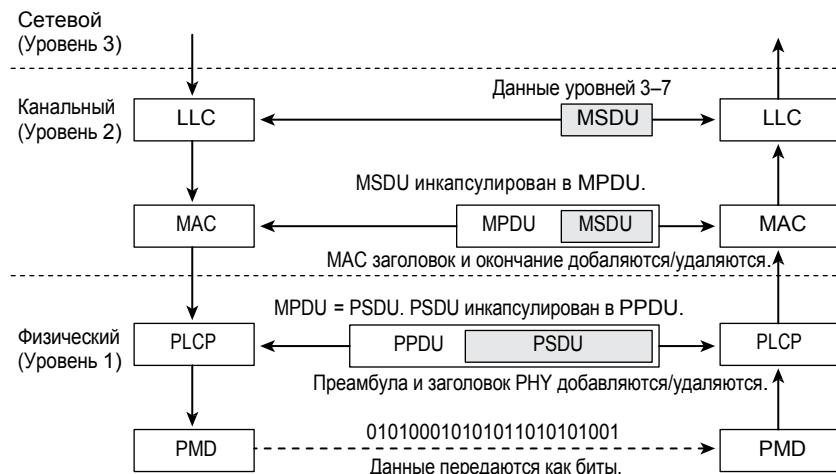
Блок сервисных данных *PLCP* [*PLCP service data unit (PSDU)*] это вид MPDU с Физического уровня. MAC уровень ссылается на кадр как на MPDU, в то время как Физический уровень ссылается на тот же самый кадр как на PSDU. Единственная разница – это с какого уровня модели OSI вы смотрите на кадр.

## Блок Данных Протокола PLCP

Когда PLCP принимает PSDU, он затем готовит PSDU к передаче, и создает *блок данных протокола PLCP* [*PLCP protocol data unit (PPDU)*]. PLCP добавляет преамбулу и заголовок PHY к PSDU. Преамбула используется для синхронизации между передающим и принимающим радиомодулями 802.11. Обсуждение всех деталей преамбулы и заголовка PHY находится за пределами этой книги и экзамена CWNA. Когда PPDU создан, подуровень PMD берет PPDU и модулирует биты данных и начинает передачу.

Рисунок 9.2 изображает диаграмму потока, который показывает движение информации верхних уровней между Канальным и Физическим уровнями.

**РИСУНОК 9.2** Канальный и Физический уровни



## 802.11 и 802.3 совместимость

Как вы узнали из Главы 7 “Топологии Беспроводных ЛВС”, стандарт 802.11-2020 определяет *сервис интеграции* [*integration service (IS)*], который делает возможным доставку MSDU между системой распространения [*distribution system (DS)*] и не IEEE-802.11 локальными вычислительными сетями (LAN), через портал. Простой способ определения сервиса интеграции – это охарактеризовать его как способ передачи формата кадра. Портал – это обычно или точка доступа, или контроллер БЛВС (WLAN). Как упоминалось ранее, полезная нагрузка беспроводного кадра данных 802.11 – это информация верхних уровней 3-7, которая называется MSDU. Итоговое назначение этой полезной нагрузки располагается в проводной сетевой инфраструктуре. Так как проводная инфраструктура – это другая физическая среда, полезная нагрузка кадра данных 802.11 (MSDU) должна быть фактически передана в кадр 802.3 Ethernet. Например, телефон VoWiFi передает кадр данных 802.11 точке доступа.

Полезная нагрузка MSDU кадра – это VoIP пакет с конечным местом назначения – сервер АТС, который находится в проводной сети. Работа сервиса интеграции – это сначала убрать заголовок 802.11 и окончание, а затем упаковать полезную нагрузку VoIP MSDU внутрь кадра 802.3 Ethernet. Обычно, сервис интеграции передает полезные нагрузки кадров между средой 802.11 и средой 802.3. Однако, IS может передавать MSDU между средой 802.11 и некоторыми видами другой среды. Все форматы кадров IEEE 802 имеют сходные характеристики, включая формат кадра 802.11. Так как кадры похожи, то это просто преобразовать кадры по мере их движения из беспроводной сети 802.11 в проводную сеть 802.3, и наоборот.

Одно из различий между кадрами 802.3 Ethernet и беспроводными кадрами 802.11 – это размер кадра. Кадры 802.3 имеют максимальный размер в 1518 байт с максимальной полезной нагрузкой данных в 1500 байт. Если кадры 802.3 с метками 802.1Q для VLANов и пользовательского приоритета, то максимальный размер кадра 802.3 – 1522 байт с полезной нагрузкой данных в 1504 байта. Как вы уже знаете, кадры 802.11 способны переносить кадры с полезной нагрузкой MSDU в 2304 байта данных верхних уровней. Это значит, что по мере движения данных между беспроводной сетью и проводной сетью, ТД может получить кадр данных, который слишком велик для проводной сети. Это редкая проблема благодаря набору протоколов TCP/IP. TCP/IP, наиболее распространенный протокол связи, используемый в сетях, обычно имеет *максимальный блок передачи IP [IP maximum transmission unit (MTU)]* размером в 1500 байт. IP пакеты обычно основаны на 1500 байтном MTU. Когда IP пакеты проходят вниз по 802.11, даже когда максимальный размер MSDU равен 2304 байта, размер будет ограничен 1500 байтами IP пакетов.

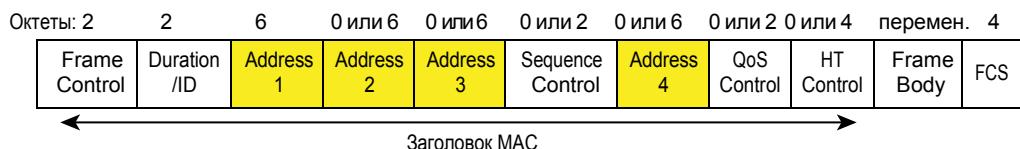
Ethernet кадры с полезной нагрузкой более чем 1500 байт называются *гигантскими кадрами [jumbo frames]* и обычно несут полезную нагрузку до 9600 байт. Многие GigabitEthernet коммутаторы и GigabitEthernet сетевые интерфейсные карты поддерживают гигантские (jumbo) кадры. БЛВСы 802.11 не поддерживают гигантские (jumbo) кадры; однако, в этом нет необходимости из-за агрегации кадров 802.11. В Главе 10, вы узнаете о более эффективных методах доставки полезной нагрузки MSDU через агрегацию кадров и A-MSDU, и A-MPDU. Пожалуйста, обратите внимание, что настройки MTU портов Ethernet некоторых БЛВС контроллеров и ТД должны быть настроены в 9000 байт, чтобы обеспечить поддержку исходящих гигантских (jumbo) кадров в проводную сеть.

## 802.11 MAC Заголовок

Каждый кадр 802.11 содержит MAC заголовок, который содержит информацию 2 уровня. Информация 2ого уровня не зашифрована и всегда видна при просмотре анализатором протоколов. Как показано на Рисунке 9.3, Заголовок MAC 802.11 имеет девять основных полей, четыре из которых используются для адресации. Оставшиеся поля включают Контрольное Поле Кадра [Frame Control], поле Длительность/ID [Duration/ID]), поле Контроля Последовательности [Sequence Control], поле контроля Качества сервиса [QoS Control], и поле Контроля Высокой Пропускной способности [HT Control]. Детальное объяснение назначение каждого поля и подполя в заголовке 802.11 MAC находится за пределами экзамена CWNA; однако, мы продолжим верхнеуровневое обсуждение некоторых из этих полей.

РИСУНОК 9.3

Заголовок MAC 802.11

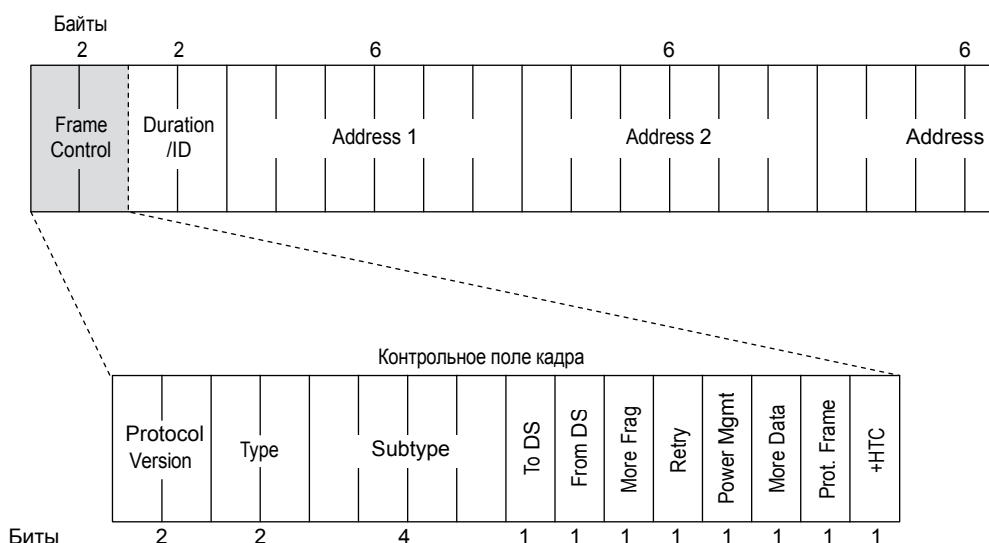


## Контрольное Поле Кадра

Первые два байта MAC заголовка состоят из 11 подполей внутри *Контрольного Поля Кадра* [*Frame Control field*]. Эти подполя включают Версию Протокола [*Protocol Version*], Тип[*Type*], Подтип[*Subtype*], К Системе Распространения[*To DS*], Из Системы Распространения [*From DS*], Есть Еще Фрагменты [*More Fragments*], Повторная Передача [*Retry*], Управление Питанием [*Power Management*], Есть Еще Данные [*More Data*], Защищенный Кадр [*Protected Frame*], и +Контроль Пропускной способности/Порядок [+*HTC/Order*]. Теперь мы обсудим некоторые из этих подполей, которые проиллюстрированы на Рисунке 9.4.

РИСУНОК 9.4

Контрольное поле кадра (Frame Control)



*Поле Версии Протокола [Protocol Version field]* - это поле из двух последовательных битов, которые всегда размещены в начале всех заголовков 802.11 MAC. Это поле просто используется для обозначения какая версия протокола технологии 802.11 используется кадром. Все кадры 802.11 имеют поле Версии Протокола всегда установленное в 0. Все другие значения являются зарезервированными. Другими словами, на текущий момент существует только одна версия технологии 802.11. Возможно, в будущем, IEEE может определить другую версию технологии 802.11, которая не будет обратно совместима с текущей версией 0.

В отличии от множества стандартов проводных сетей, таких как IEEE 802.3, которые используют единый тип кадра данных, стандарт IEEE 802.11-2020 определяет три основных типа кадров: управление [*management*], контроль [*control*], и данные [*data*]. Эти типы кадров 802.11 далее подразделяются на несколько подтипов. В действительности, определено четыре типа кадров 802.11, расширенных кадров [*extension frames*]. Расширенные кадры используются в радиомодулях 802.11ad - направленном мультигигабите [*directional multi-gigabit (DMG)*], который работает на 60ГГц, или в радиомодулях 802.11ah, которые работают ниже 1 ГГц [*sub 1 GHz (S1G)*]. Обсуждение расширенных кадров 802.11 находится за пределами экзамена CWNA. Поле Тип заголовка 802.11 определяет является ли кадр – кадром управления, кадром контроля, кадром данных или расширенным кадром. Как показано в Таблице 9.1, 2x-битное поле Тип определяет является ли кадр контрольным, кадром данных, кадром управления или расширенным кадром. Значение 00 означает – кадр управления, значение 01 – обозначает контрольный кадр, значение 10 – кадр данных, и значение 11 обозначает расширенный кадр.

**ТАБЛИЦА 9.1** Типы кадров 802.11

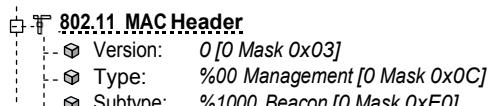
Биты	Тип Кадра	Назначение
00	Management (Управление)	Используется для обнаружения ТД и присоединения к BSS
01	Control (Контроль)	Используется для подтверждения успешной передачи и резервирования беспроводной среды
10	Data (Данные)	Используется для переноса полезной нагрузки MSDU верхних уровней
11	Extension (Расширение)	Гибкий формат кадра, на текущий момент используется только в радиомодулях DMG (802.11ad) или S1G (802.11ah)



Не перепутайте кадры управления, контроля и данных с тремя плоскостями (*plane*) телекоммуникаций с такими же названиями. Обсуждение плоскостей (*planes*) управления, контроля и данных по отношению к работе архитектуры БЛВС сети можно найти в Главе 11 “Архитектура БЛВС”.

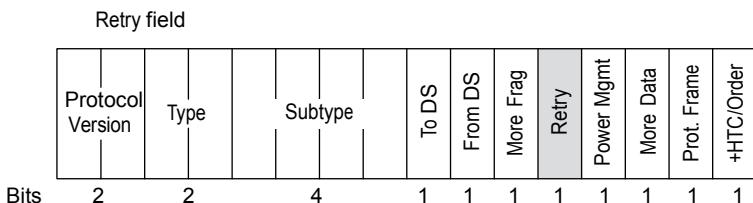
Поле *Typ* [*Type field*] и поле *Подтип* [*Subtype field*] используются вместе, чтобы идентифицировать функцию кадра. Из-за того, что существует множество различных видов кадров управления, контроля и данных, требуется 4x-битное поле Подтипа. Например, Рисунок 9.5 показывает часть перехваченного кадра управления. Поле Подтип показывает, что кадр является кадром управления - маяком [*beacon*].

**РИСУНОК 9.5** Поля Тип и Подтип



*Поле Повторной передачи или Повтора [Retry field]* это один значащий бит информации находящийся во всех МАС заголовках. Поле Повтора содержит один бит Контрольного Поля Кадра, и, пожалуй, является одним из наиболее важных полей в заголовке МАС. Если бит Повтора[Retry] имеет значение 0, то имеет место быть первоначальная передача. Если бит Повтора [Retry] установлен в значение 1 в кадре управления или кадре данных, передающий радиомодуль показывает, что кадр посыпается как повторная передача. Рисунок 9.6 показывает положение поля Повтор в заголовке МАС.

**РИСУНОК 9.6**      Поле повтор (повторная попытка)



Как обсуждалось много раз в этой книге, каждый раз, когда радиомодуль 802.11 передает однородный [unicast] кадр, и если кадр принят целым и прошла циклическая проверка избыточности (CRC) последовательности проверки кадра (FCS), то радиомодуль 802.11, который получил кадр, ответит кадром подтверждения [acknowledgment (ACK)]. Если ACK получено, исходная станция знает, что передача кадра была успешна. Если любая часть однородного[unicast] кадра повреждена, CRC не пройдет, и приемный радиомодуль 802.11 не отправит кадр ACK передающему радиомодулю 802.11. Если кадр ACK не получен исходным передающим радиомодулем, однородный [unicast] кадр не подтвержден, и должен быть повторно передан. Бит Повтора [Retry] является показателем, что передаваемый кадр является повторной передачей, а не исходной передачей кадра. Любой хороший анализатор протокола 802.11 может вывести скорость повторных передач 2 уровня наблюдая за кадрами управления и данных, у которых поле Повтора [Retry] установлено в значение 1.

*Поле Защищенного Кадра [Protected Frame field]* это один бит, и используется для обозначения зашифрована ли полезная нагрузка MSDU кадра данных. Поле Защищенного Кадра является подполем Контрольного Поля Кадра [Frame Control field]. Когда поле Защищенный Кадр установлено в значение 1 в кадре данных, то полезная нагрузка MSDU кадра данных действительно зашифрована. Поле Защищенный Кадр не обозначает какой тип шифрования используется, он показывает только, что полезная нагрузка MSDU кадра данных зашифрована. Шифрование может быть Проводным Эквивалентом Секретности [Wired Equivalent Privacy (WEP)], Протоколом Целостности Временных Ключей [Temporal Key Integrity Protocol (TKIP)], или Режима Счетчика с Протоколом Шифровальных Блоков Цепочки Сообщения Аутентификационного Кода [Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)].

## Поле Длительность/Идентификатор (Duration/ID)

Очень важное поле, которое обсуждалось ранее в этой книге – *Поле Длительность/Идентификатор [Duration/ID field]*. Как вы узнали из Главы 8 “Доступ к Среде 802.11”, значение длительности в заголовке MAC передающей станции используется для переустановки таймера NAV других слушающих станций.

Для повторения, виртуальный контроль несущей использует механизм таймера, называемого *вектор сетевого распределения [network allocation vector (NAV)]*. Таймер NAV управляет предсказанием будущего трафика в среде на основе информации значения Длительности [Duration], увиденной в предыдущей передаче кадра. Когда радиомодуль 802.11 не передает, он слушает. Когда слушающий радиомодуль слышит передачу кадра от другой станции, он смотрит в заголовок кадра. Затем приемник определяет содержит ли поле Duration/ID значение Длительности [Duration] или значение Идентификатора (ID). Если поле содержит значение Длительности [Duration], то слушающая станция установит свой таймер NAV в это значение. Затем слушающая станция будет использовать NAV как таймер обратного отсчета, зная, что радиосреда будет занята, пока отсчет не достигнет 0.

Это поле почти всегда используется для информации о значении длительности для виртуального контроля несущей, как только что упоминалось. Однако, второй способ трактовки поля Duration/ID используется во время старых процессов управления питанием. Во время этого процесса, клиенты используют поле в контрольном кадре PS-Poll (кадре опроса при энергосбережении) в качестве идентификатора для ТД во время процесса управления электропитанием. Более детальное обсуждение об управлении питанием следует далее в этой главе.

## Адресация MAC уровня

Почти как в кадре 802.3 Ethernet, заголовок кадра 802.11 содержит MAC адреса. MAC адрес бывает одним из следующих типов:

**Индивидуальный Адрес** Индивидуальные адреса назначаются уникальным станциям на сети (также называются как *однонаправленный адрес [unicast address]*).

**Групповой Адрес** Адрес с несколькими назначениями или адресатами (групповой адрес) может быть использован одной или более станциями на сети. Существуют два вида групповых адресов:

**Адрес Многоадресной (Multicast)-Группы** Адрес, используемый верхнеуровневыми объектами для определения логической группы станций, называется как *адрес многоадресной группы [multicast-group address]*.

**Широковещательный(Broadcast) Адрес** Групповой адрес, который обозначает все станции, которые принадлежат сети, называется *широковещательным адресом [broadcast address]*. Широковещательный адрес, все биты которого имеют значение 1, определяет все станции в локальной вычислительной сети. В шестнадцатеричном исчислении, широковещательный адрес будет FF:FF:FF:FF:FF:FF.

Хотя и есть схожести, MAC адресация, используемая кадрами 802.11 намного более сложная чем Ethernet кадрами. Кадры 802.3 имеют только адрес источника [source address (SA)] и адрес назначения [destination address (DA)] в заголовке 2 уровня. Как показано ранее на

Рисунок 9.3, кадры 802.11 содержат до четырех полей адресов в MAC заголовке. Кадры 802.11 обычно используют только три MAC-адресных поля. Однако, кадр 802.11, отправленный в беспроводную систему распространения [wireless distribution system (WDS)] требует все четыре MAC адреса. Определенные кадры могут не содержать некоторые адресные поля. Несмотря на то, что число адресных полей различно, и 802.3 и 802.11 определяют адрес источника и адрес назначения, и используют один и тот же формат MAC адреса. Первые три октета в MAC адресе называются *уникальным идентификатором организации [organizationally unique identifier (OUI)]*, а последние три октета называются дополнительным или добавочным идентификатором [*extension identifier*].

Как показано на Рисунке 9.7, существуют четыре поля MAC адресов 802.11: Адрес 1 (Address 1), Адрес 2 (Address 2), Адрес 3(Address 3), и Адрес4 (Address 4). В зависимости от того, как используются поля К Системе Распространения (To DS) И Из Системы Распространения (From DS), определение каждого из четырех полей MAC адресов будет меняться. Существует пять возможных определений:

**Адрес Источника [Source Address (SA)]** MAC адрес изначальной отправляющей станции, называется адресом источника [*source address (SA)*]. Адрес источника может начинаться как с беспроводной станции, так и с проводной сети.

**Адрес Назначения [Destination Address (DA)]** MAC адрес конечного назначения кадра на 2ом уровне называется *адресом назначения [destination address (DA)]*. Конечное назначение может быть беспроводной станцией или получателем в проводной сети, таким как сервер.

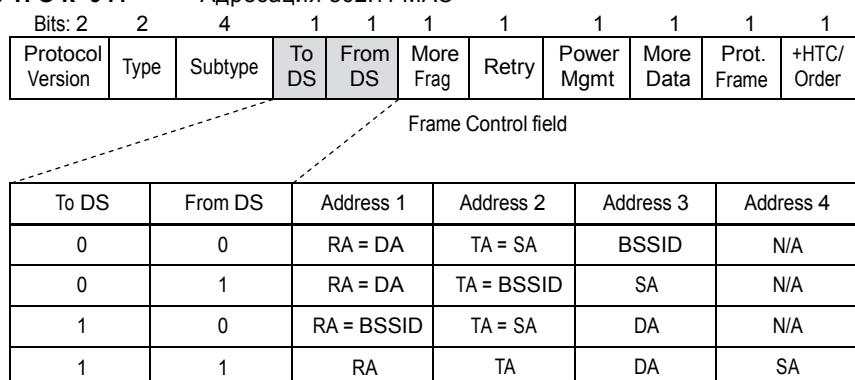
**Адрес Передатчика [Transmitter Address (TA)]** MAC адрес радиомодуля 802.11, который передает кадр в полудуплексную среду 802.11 называется *адресом передатчика [transmitter address (TA)]*.

**Адрес Приемника [Receiver Address (RA)]** MAC адрес радиомодуля 802.11, который предназначен для получения входящей передачи от передающей станции называется *адресом приемника [receiver address (RA)]*.

**Идентификатор Базового Состава Сервиса [Basic Service Set Identifier (BSSID)]**

Это MAC адрес, который является идентификатором 2 уровня базового состава сервиса (BSS). *Идентификатор базового состава сервиса [basic service set identifier (BSSID)]* это MAC адрес радиомодуля ТД, или выведенный из MAC адреса радиомодуля ТД, если присутствует несколько базовых составов сервиса.

**Р И С У Н О К 9 . 7** Адресация 802.11 MAC



- SA = MAC адрес исходного отправителя (проводного или беспроводного)
- DA = MAC адрес конечного назначения (проводного или беспроводного)
- TA = MAC адрес передающего радиомодуля 802.11
- RA = MAC адрес принимающего радиомодуля 802.11
- BSSID = L2 идентификатор базового состава сервиса (BSS)

Поле "К Системе Распространения" [To DS] и поле "Из Системы Распространения" [From DS] каждое является 1 битным и используются совместно для изменения назначений четырех MAC адресов в заголовке 802.11. Эти два бита также показывают поток кадров данных 802.11 между БЛВС средой и системой распространения [DS]. DS обычно является проводной средой Ethernet. В зависимости от того как поля «To DS» и «From DS» используются вместе с четырьмя MAC адресами, определение каждого поля изменится. Однако, есть одно постоянство - это то, что поле Адрес 1(Address 1) всегда будет адресом приемника [receiver address (RA)], но может иметь и второе определение также. Адрес 2 (Address 2) всегда будет адресом передатчика [transmitter address (TA)], но также может иметь второе определение. Адрес 3 (Address 3) обычно используется для информации о дополнительном MAC адресе. Адрес (Address 4) используется только в случае WDS.

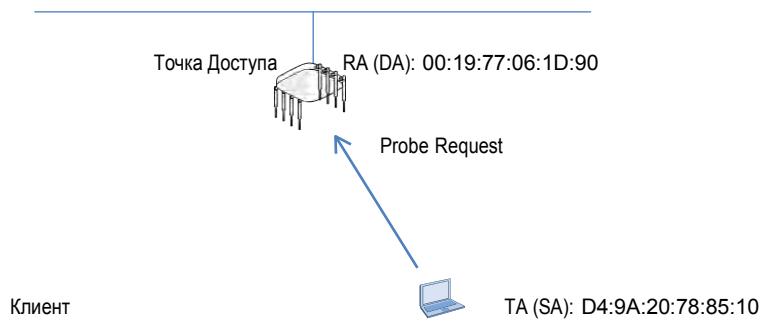
Существует четыре возможные комбинации этих двух битов. Первая комбинация битов «To DS» и «From DS» следующая:

To DS = 0  
From DS = 0

Когда оба бита установлены в 0, могут существовать несколько разных сценариев. Наиболее общий сценарий – это то, что это кадры управления или контроля. Кадры управления и контроля не имеют полезной нагрузки MSDU, поэтому их конечный пункт назначения никогда не является системой распространения(distribution system (DS)). Кадры управления и контроля существуют только на MAC подуровне, и следовательно, не должны быть преобразованы сервисом интеграции [integration service (IS)], и никогда не посыпаются в проводную среду. Рисунок 9.8 изображает MAC адресацию, используемую для кадра управления зондирующем запросом [probe request management frame], посланного клиентом к ТД. Третье адресное поле несет дополнительную информацию, и используется для идентификации BSSID. Адресные поля 1 и 3 имеют тоже самые значения, потому что ТД является и адресом приемника (RA) и BSSID. Рисунок 9.9 изображает MAC адресацию, используемую для кадра управления с зондирующими ответом [probe response management frame], отправленного ТД к клиенту. Адресные поля 2 и 3 имеют одно и то же значение, потому что ТД является и адресом передатчика (TA) и BSSID.

**Р И С У Н О К 9 . 8**

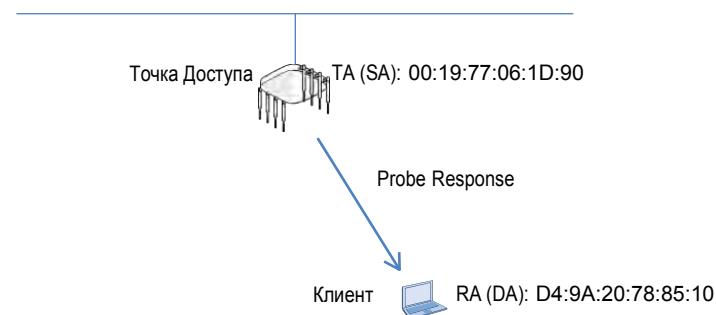
To DS=0, From DS=0 Зондирующий запрос (Probe request)

*To DS: 0 From DS: 0*

Адрес #1: RA (DA): 00:19:77:06:1D:90  
 Адрес #2: TA (SA): D4:9A:20:78:85:10  
 Адрес #3: BSSID: 00:19:77:06:1D:90

**Р И С У Н О К 9 . 9**

To DS:0 From DS:0 Зондирующий ответ(Probe response)

*To DS: 0 From DS: 0*

Адрес #1: RA (DA): D4:9A:20:78:85:10  
 Адрес #2: TA (SA): 00:19:77:06:1D:90  
 Адрес #3: BSSID: 00:19:77:06:1D:90

Другой сценарий, когда оба DS бита установлены в 0 – это прямая передача кадра данных от одной STA к другой STA в независимом базовом составе сервиса (IBSS), более известном по имени сеть ad hoc или сеть "на лету". Третий сценарий включает, что называется канал связи станция-станция [station-to-station link (STSL)], который включает отправку кадров данных прямо от одной клиентской станции к другой клиентской станции, которые принадлежат одному и тому же BSS, таким образом проходя мимо ТД.

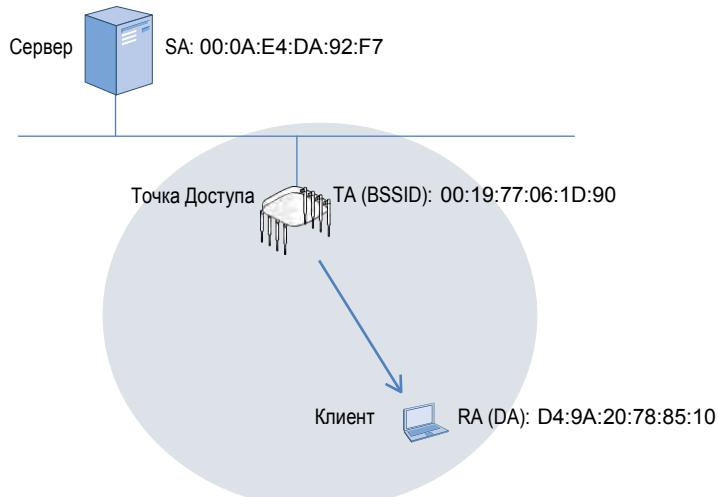
Вторая комбинация битов «To DS» и «From DS» :

To DS = 0

From DS = 1

Биты «To DS» и «From DS» могут быть использованы для обозначения направления и потока кадров данных 802.11 в обычном BSS. Когда бит «To DS» установлен в 0, а бит «From DS» установлен в 1, это показывает, что кадр данных 802.11 отправлен в нисходящем канале связи [downlink] от точки доступа к клиентской станции. Исходный источник полезной нагрузки MSDU кадра данных 802.11 является адресом, который существует в проводной сети. Как показано на Рисунке 9.10, примером может быть DHCP сервер, находящийся в сети 802.3 и отправляющий предложение DHCP по использованию IP адреса [DHCP lease offer] через ТД с конечным назначением – клиентской станцией 802.11. Адрес радиомодуля точки доступа - 00:19:77:06:1D:90, а адрес клиентской станции - D4:9A:20:78:85:10. Адрес DHCP сервера, который находится в сети 802.3 - 00:0A:E4:DA:92:F7. Поле «Адрес 1» всегда является адресом приемника [receiver address (RA)], которое является клиентской станцией и конечным адресом назначения [final destination address (DA)]. Поле «Адрес 2» всегда является адресом передатчика [transmitter address (TA)] и является точкой доступа, которая также является BSSID. Поле «Адрес 3» несет дополнительную информацию, и используется для идентификации адреса источника [source address (SA)] DHCP сервера, который существует в среде 802.3

**Р И С У Н О К 9 . 1 0** To DS:1 From DS:0 – Нисходящий (Downlink) трафик



*To DS: 0 From DS: 1*

Адрес #1: RA (DA): D4:9A:20:78:85:10  
 Адрес #2: TA (BSSID): 00:19:77:06:1D:90  
 Адрес #3: SA: 00:0A:E4:DA:92:F7

Третья комбинация битов «To DS» и «From DS»:

To DS = 1

From DS = 0

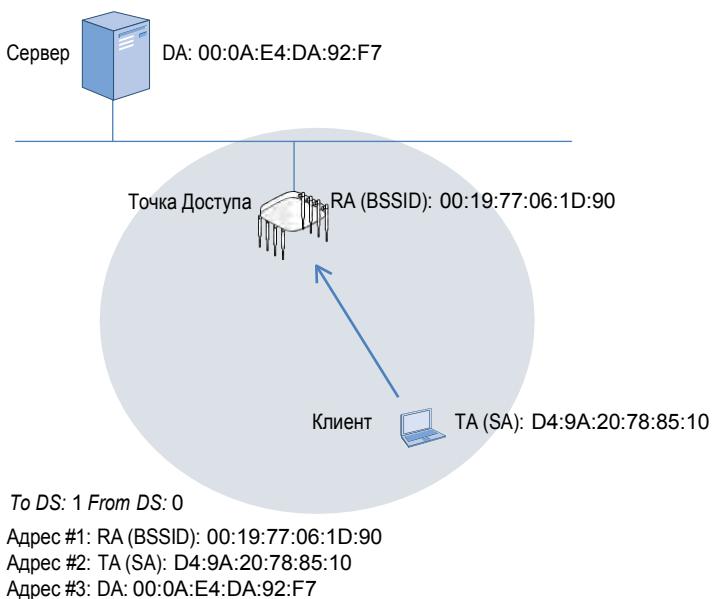
Когда бит «To DS» установлен в 1, а бит «From DS» установлен в 0, это показывает, что кадр данных 802.11 отправлен в восходящем канале связи [uplink] от клиентской станции к точке доступа. В большинстве случаев, конечным назначением полезной нагрузки MSDU кадра данных является адрес, который находится в проводной сети. Как показано на Рисунке 9.11, примером этого сценария будет клиентская станция, отправляющая пакет с DHCP запросом [DHCP request] через ТД к DHCP серверу, который находится в сети 802.3. Адрес DHCP сервера, который находится в проводной сети - 00:0A:E4:DA:92:F7. Поле «Адрес 1» всегда является адресом приемника (RA), который является радиомодулем точки доступа и BSSID. Поле «Адрес 2» всегда является адресом передатчика (TA) и является клиентской станцией, которая также является адресом источника (SA). Поле «Адрес 3» несет дополнительную информацию, и используется для идентификации адреса назначения (DA) DHCP сервер, который находится в среде 802.3.

Четвертая комбинация битов «To DS» и «From DS»:

To DS = 1

From DS = 1

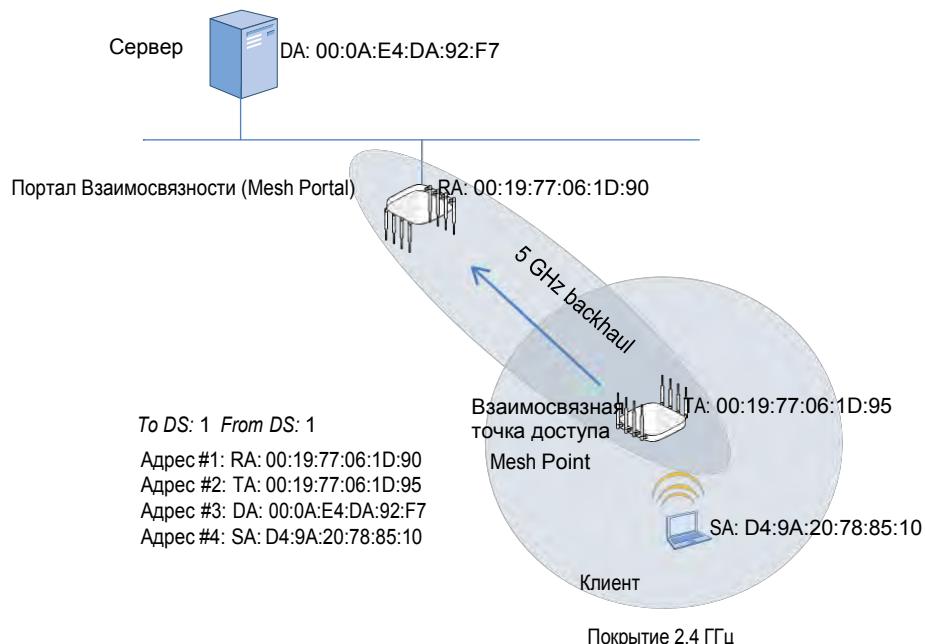
**Р И С У Н О К 9.11** To DS:1 From DS:0 – Восходящий (Uplink) трафик



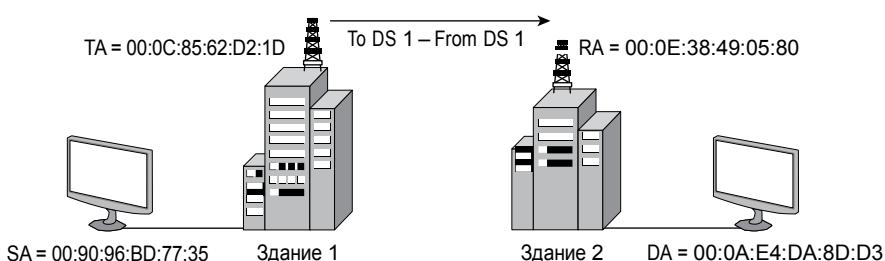
Когда бит «To DS» и бит «From DS» оба установлены в 1, это единственное время, когда кадры данных используют четырех адресный формат. Хотя стандарт не определяет процедуры по использованию этого формата, производители БЛВС часто применяют, что называется, беспроводную систему распространения [*wireless distribution system (WDS)*]. Примеры WDS -это БЛВС мосты и сети с поддержкой взаимосвязности [mesh]. В этих сценариях WDS, кадр данных отправляется через вторую беспроводную среду, прежде чем, в итоге, быть отправленным в проводную среду. Когда поля «To DS» и «From DS» оба установлены в значение 1, используется WDS, и нужно четыре адреса.

Рисунок 9.12 показывает пример 5ГГц транзитного [backhaul] канала 802.11 с поддержкой взаимосвязности [mesh] между точкой взаимосвязности [mesh point] и порталом взаимосвязности [mesh portal]. Клиентская станция, ассоциированная с 2,4ГГц радиомодулем точки доступа с поддержкой взаимосвязности [mesh], хочет отправить кадр на сервер, который находится в опорной сети 802.3. Когда кадр пересыпается через 5ГГц беспроводную магистраль, биты «To DS» и «From DS» оба установлены в 1, и нужно четыре адреса. Поле «Адрес 1» всегда является адресом приемника (RA), который в этом случае является 5ГГц радиомодулем портала взаимосвязности [mesh]. Поле «Адрес 2» всегда является адресом передатчика (TA), который в этом примере является 5ГГц радиомодулем точки взаимосвязности [mesh]. Поле «Адрес 3» содержит адрес назначения (DA), который является сервером в проводной среде. Поле «Адрес 4» является адресом источника, который является клиентской станцией, которая ассоциирована с 2,4ГГц радиомодулем точки доступа с поддержкой взаимосвязности [mesh]. Из этого примера вы можете увидеть, зачем нужны четыре адреса в транзитном взаимосвязном канале [mesh backhaul], который является беспроводной системой распространения (WDS).

Рисунок 9.13 показывает пример моста точка-точка 802.11 между двумя зданиями. Кадр нужно отправить от проводного сервера в здании 1 к проводному настольному компьютеру в здании 2. Поле «Адрес 1» всегда является адресом приемника (RA), который в этом случае является БЛВС мостом в здании 2. Поле «Адрес 2» всегда является адресом передатчика (TA), который в этом примере является БЛВС мостом в здании 1. Поле «Адрес 3» содержит адрес назначения (DA), которое является настольным компьютером в здании 2, а поле «Адрес 4» является

**Р И С У Н О К 9 .1 2** To DS:1 From DS:1 – Взаимосвязный транзитный канал [Mesh backhaul]**Р И С У Н О К 9 .1 3** To DS:1 From DS:1 – Канал связи - мост БЛВС**802.11 MAC Header**

Version:	0
Type:	%10 Data
Subtype:	%1000 QoS Data
Frame Control Flags:	%00000011
Duration:	44 Microseconds
Receiver:	00:0E:38:49:05:80
Transmitter:	00:0C:85:62:D2:1D
Destination:	00:0A:E4:DA:8D:D3
Source:	00:90:96:BD:77:35
Seq Number:	982
Frag Number:	0



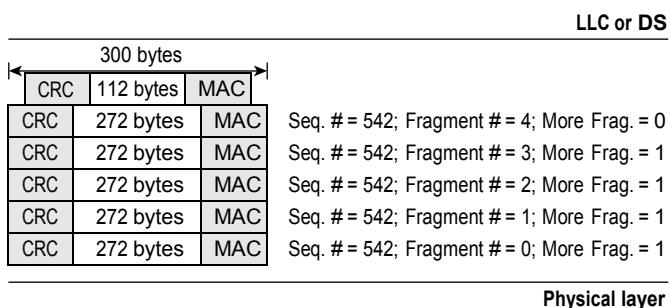
адресом источника, который является настольным компьютером в здании 1. Из этого примера, вы можете увидеть почему четыре адреса нужны в беспроводном мосте для беспроводного канала БЛВС, который является WDS.

## Поле Контроля Последовательности

*Поле Контроля Последовательности [Sequence Control field]* - это 16 битное поле содержащее два подполя, и используется когда MSDU 802.11 фрагментируется. Стандарт 802.11-2020 допускает фрагментацию кадров. *Фрагментация [Fragmentation]* разбивает кадр 802.11 на меньшие части, называемые фрагментами, добавляет заголовок к каждому фрагменту, и передает каждый фрагмент отдельно. На всех ТД 802.11 и некоторых станциях-клиентах могут быть настроены пороги фрагментации [fragmentation threshold]. Если порог фрагментации установлен в 300 байт, то любой MSDU больше чем 300 байт будет фрагментирован. Рисунок 9.4 изображает 1200 байтный MSDU с номером последовательности 542.

Основываясь на пороге 300 байт, Рисунок 9.14 показывает фрагментацию снизу вверх, потому что фрагменты двигаются вниз по стэку OSI. Информация, показанная в поле Контроля Последовательности, также нужна приемному радиомодулю, чтобы снова собрать фрагменты.

**Р И С У Н О К 9 . 1 4**      Фрагментация



Хотя передано тоже самое количество реальных данных, фрагментация вносит дополнительную служебную информацию на MAC уровне, так называемый оверхед [overhead] или дополнительные накладные расходы. Каждый фрагмент требует свой собственный заголовок и окончание, а за передачей каждого кадра следует короткое межкадровое пространство [short interframe space (SIFS)] и подтверждение (ACK). В правильно работающей сети 802.11, более мелкие фрагменты действительно уменьшают пропускную способность передачи данных из-за накладных расходов дополнительного заголовка MAC подуровня, SIFS, и ACK каждого кадра. С другой стороны, если сеть испытывает большое количество поврежденных данных, уменьшение значения в настройках фрагментации 802.11 может улучшить пропускную способность передачи данных. Фрагменты всегда посылаются в, так называемом, *фрагментном взрыве* [*fragment burst*]. Фрагментация иногда использовалась в устаревших сетях 802.11a/b/g, но больше не нужна в сетях 802.11n/ac/ax, которые поддерживают агрегацию кадров и Блоковые подтверждения (Block ACKs). Так как фрагментация редко используется, глубокое обсуждение фрагментации находится за пределами экзамена CWNA.



Передача фрагментов осуществляется таким же способом, как и передача кадра. Следовательно, каждый фрагмент должен участвовать в доступе к среде CSMA/CA и за которым должно следовать подтверждение (ACK). Если за фрагментом не следует ACK, он будет передан повторно.

## Поле Контроля Качества Сервиса (QoS)

Поле Контроля Качества Сервиса [*QoS Control field*] это 16 битное поле, которое определяет параметры качества сервиса [*quality-of-service (QoS)*] кадра данных. Заметьте, что не все кадры данных содержат поле Контроля Качества Сервиса. Поле Контроля Качества [*QoS Control field*] используется только в MAC заголовке кадров передачи данных с качеством сервиса. Как вы узнали в Главе 8, в проводной среде 802.3 Ethernet, доступны различные классы сервиса, представленные в 3х битном поле Пользовательского Приоритета [*User Priority*] в заголовке 802.1Q, добавленном к кадру Ethernet. 802.1D делает возможным очередизацию по приоритетам (позволяя некоторым кадрам Ethernet быть отправленными раньше других в коммутируемой сети Ethernet). Эти классы сервиса 802.1D поставлены в соответствие с категориями доступа *Wi-Fi Мультимедиа* [*Wi-Fi Multimedia (WMM)*]. WMM обеспечивает приоритезацию трафика в 802.11 по четырем категориям доступа: голос [*voice*], видео [*video*], данные без гарантированной доставки [*best effort*], и фоновые данные [*background*]. Поле Контроля Качества Сервиса [*QoS Control field*] иногда называется как поле Контроля Качества Сервиса WMM [*WMM QoS Control field*], потому что поле Контроля QoS фактически показывает класс сервиса WMM кадра данных с качеством сервиса [*QoS data frame*].

## Поле Контроля Высокой Пропускной Способности (HT)

Поле Контроля Высокой Пропускной Способности [*HT Control field*] используется для адаптации канала связи [*link adaptation*], формирования луча передачи [*transmit beamforming (TxBF)*], и других улучшенных возможностей передатчиков и приемников 802.11n/ac/ax. Поле Контроля Высокой Пропускной Способности [*HT Control field*] используется только в кадрах управления и кадрах передачи данных с качеством-сервиса

(QoS), когда подполе +HTC поля Контроля Кадра установлено в значение 1. Полное объяснение Поля Контроля Высокой Пропускной Способности [HT Control field] находится за пределами экзамена CWNA.



Хотя мы в значительной степени охватили заголовок 802.11 MAC, объяснение назначение каждого поля и под поля заголовка MAC 802.11, также, как и назначение всех фиксированных полей и информационных элементов, используемых в многочисленных кадрах 802.11 управления, контроля и данных, находится за рамками экзамена CWNA. Для глубокого рассмотрения формата кадра 802.11, мы рекомендуем вам прочитать (*CWAP Сертифицированный Профессионал по Беспроводному Анализу, Официальное Учебное Пособие: Экзамен PW0-270 (Sybex, 2011)* - *CWAP Certified Wireless Analysis Professional Official Study Guide: Exam PW0-270 (Sybex, 2011)*).

## Тело Кадра 802.11

Как вы уже знаете, существует три основных типа кадров 802.11: управление, контроль и данные. Следует отметить, что не все три типа кадров несут один и тот же тип полезной нагрузки в теле кадра. Суть в том, что кадры контроля не имеют тела.

Другое название кадра управления 802.11 – *блок данных управления протокола MAC [management MAC protocol data unit (MMPDU)]*. У кадров управления есть MAC заголовок, тело кадра, и окончание; однако, кадры управления не несут никакую информацию верхних уровней. Нет никакой инкапсулированного MSDU в теле кадра MMPDU, который несет только информационные поля и элементы 2 уровня.

*Информационные поля [Information fields]* являются обязательными полями фиксированной длины в теле кадра управления. *Информационные элементы [Information elements]* – переменной длины и опциональны (т.е. необязательны). Примером информационного элемента может быть *информационный элемент RSN [RSN information element]*, который содержит информацию о типе аутентификации и шифровании, используемом в BSS. Полезная нагрузка в теле кадра MMPDU не зашифрована. Мы обсудим различные подтипы кадров управления 802.11 позже в этой главе.

Контрольные кадры используются, чтобы очистить канал, занять канал, и обеспечить подтверждениями односторонние [unicast] кадры. Они содержат только заголовок и окончание. У контрольных кадров нет тела кадра. Мы также обсудим различные подтипы контрольных кадров 802.11 позже в этой главе.

Только кадры данных 802.11 несут полезную нагрузку MSDU верхних уровней в теле кадра. Когда используется шифрование, полезная нагрузка MSDU защищена. Обратите внимание, что определенные подтипы кадров данных, таких как кадр нулевого действия или функции (null function frame), не имеют тела кадра. Мы также обсудим различные подтипы кадров данных 802.11 позже в этой главе.

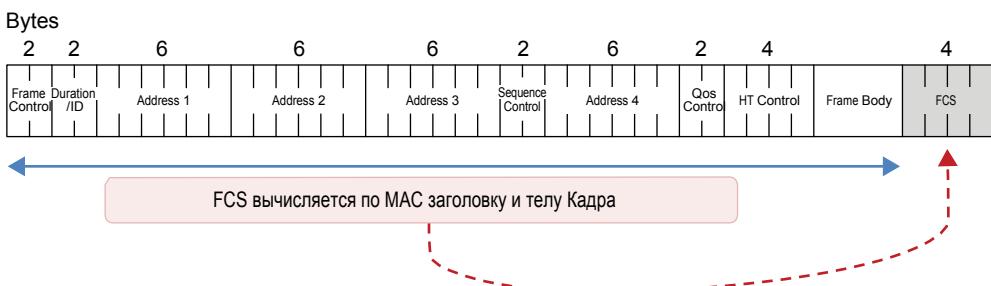
## Окончание 802.11

Главное назначение окончания 802.11 – это нести информацию для проверки целостности данных для каждого кадра. Находящаяся в каждом окончании 802.11 *последовательность проверки кадра [frame check sequence (FCS)]*, также называется, как *поле FCS [FCS field]*, которое содержит 32x битную циклическую избыточную проверку (cyclic redundancy

### 342 Глава 9 • 802.11 MAC

check (CRC)), которая используется для подтверждения целостности полученного кадра. Как показано на Рисунке 9.5, FCS вычисляется по всем полям MAC заголовка и поля Тела Кадра. Они называются *вычислительные поля [calculation fields]*.

**РИСУНОК 9.15** Последовательность проверки кадра (Frame check sequence)



FCS вычисляется, используя следующий стандартный образующий многочлен степени 32:

$$G(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$$

Вам нужно полностью понимать эту формулу для экзамена CWNA. (Шутка!) Что вам абсолютно нужно понимать для экзамена – это то, что произойдет, если CRC не пройдет или пройдет, когда однокомандный кадр получен станцией 802.11. Как упоминалось ранее в этой главе, каждый раз, когда радиомодуль 802.11 передает однокомандный кадр, если кадр принят правильно, и циклическая избыточная проверка (CRC) FCS пройдена, радиомодуль 802.11, который получил кадр, ответит кадром подтверждения (ACK). Если подтверждение(ACK) получено, исходная станция знает, что передача кадра была успешной. Все однокомандные [unicast] кадры 802.11 должны быть подтверждены. Широковещательные [Broadcast] и многоадресные [multicast] кадры не требуют подтверждения.

Если любая часть однокомандного [unicast] кадра повреждена, CRC не пройдет, а принимающий радиомодуль 802.11 не отправит кадр ACK передающему радиомодулю 802.11. Если кадр ACK не получен исходным передающим радиомодулем, однокомандный кадр считается неподтвержденным, и должен быть отправлен повторно.

# Машина Состояний 802.11

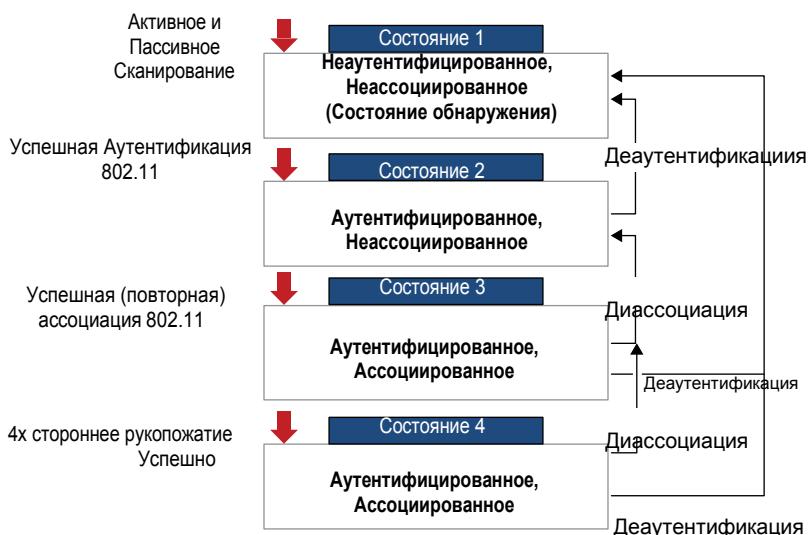
Стандарт 802.11-2020 определяет четыре состояния подключения клиента. Эти четыре состояния часто называются *машиной состояний 802.11 [802.11 state machine]*. Обмен кадрами управления 802.11 используется между станцией клиентом и ТД по мере перехода клиента между четырьмя состояниями для установления соединения 2ого уровня. Вот эти четыре состояния:

- Состояние 1: Начальное стартовое состояние, неаутентифицированное и неассоциированное
- Состояние 2: Аутентифицированное, неассоциированное
- Состояние 3: Аутентифицированное и ассоциированное (с ожидание RSN аутентификации)
- Состояние 4: Аутентифицированное и ассоциированное

Назначение машины состояний 802.11 в том, чтобы сделать возможным для клиентов и ТД обнаруживать друг друга, и устанавливать безопасное взаимодействие, с конечной целью присоединения клиента к базовому составу сервиса (BSS). Если не используется никакая безопасность, то нужны только три состояния. В большинстве случаев, требуется аутентификация PSK или 802.1X/EAP, и тогда имеют место быть все четыре состояния.

Рисунок 9.16 иллюстрирует обмен кадров управления, которое происходит между этими состояниями. В следующем разделе, мы обсудим более детально все кадры управления, которые используются между клиентской станцией и ТД при присоединении и покидании BSS.

**Р И С У Н О К 9 . 1 6**      Машина состояний 802.11



# Кадры Управления

Внутри любого BSS, большой процент трафика БЛВС состоит из *кадров управления 802.11* [802.11 *management frames*]. Кадры управления используются беспроводными станциями чтобы присоединится к и покинуть базовый состав сервиса [basic service set (BSS)]. Они не нужны в проводной сети, так как физическое подключение и отключение сетевого кабеля выполняет эту функцию. Однако, из-за того, что беспроводная сеть является неограниченной средой, беспроводной станции необходимо сначала найти совместимую БЛВС, затем аутентифицироваться в БЛВС (предполагая, что они разрешают подключиться), и затем ассоциироваться с БЛВС (обычно с ТД), чтобы получить доступ к проводной сети (системе распространения). В большинстве случаев, также требуется безопасность RSN.

Другое называние кадров управления 802.11 – *блок данных протокола управления MAC* [*management MAC protocol data unit (MMPDU)*]. Кадры управления не несут никакой информации верхних уровней. Нет инкапсулированного MSDU в теле кадра MMPDU, который несет только информационные поля и информационные элементы 2 уровня. Информационные поля – это поля фиксированной длины в теле кадра управления. Информационные элементы имеют переменную длину.

Далее идет список всех 14 подтипов кадров управления, определенных стандартом 802.11 и принятыми поправками:

- Запрос на ассоциацию [Association request]
- Ответ на ассоциацию [Association response]
- Запрос на повторную ассоциацию или переассоциацию [Reassociation request]
- Ответ на запрос на переассоциацию [Reassociation response]
- Зондирующий запрос [Probe request]
- Зондирующий ответ или Ответ на зондирующий запрос [Probe response]
- Маяк [Beacon]
- Сообщение, показывающее о наличии трафика [Announcement traffic indication message (ATIM)]
- Деассоциация [Disassociation]
- Аутентификация [Authentication]
- Деаутентификация [Deauthentication]
- Действие [Action]
- Действие без Подтверждения [Action No ACK]
- Синхронизационные оповещения [Timing advertisement]

Сейчас мы обсудим наиболее употребительные кадры управления 802.11.

## Маяк (Beacon)

Один из самых важных типов кадров 802.11 – это *маяк* [*beacon*], также называемый как *кадр управления - маяк* [*beacon management frame*]. Маяки [Beacons] фактически являются сердцебиением беспроводной сети. ТД базового состава сервиса осуществляет широковещание маяков, а клиенты слушают кадры маяки.

Клиентские станции передают маяки только когда участвуют в независимом базовом составе сервиса [independent basic service set (IBSS)], также называемом режиме ad hoc или "на лету". Каждый маяк содержит отметку времени [time stamp], которую клиентские станции используют, чтобы поддерживать свои часы синхронизированными с ТД. Так как так много успешной беспроводной связи, основанной на синхронизации [timing], безусловно, что все станции будут синхронизированы друг с другом. Выполняя Упражнение 9.1, вы сможете проинспектировать содержание кадра маяка, используя анализатор беспроводных пакетов. Более 75 фиксированных полей и информационных элементов может быть в кадре Маяка, в зависимости от рабочего режима точки доступа. Таблица 9.2 включает частичный список информации, которая может находиться в теле кадра-маяка.

**ТАБЛИЦА 9.2** Содержание кадра-маяка

Тип Информации	Описание
Отметка Времени [Time Stamp]	Синхронизационная информация
Интервал маяка [Beacon Interval]	Число временных единиц (time units (TUs)) между временем целевой передачи маяка (target beacon transmission times (TBTTs))
SSID	Логическое имя БЛВС
Скорости передачи данных	Базовая и поддерживаемые скорости передачи данных
Возможности Сервисного Состава [Service Set capabilities]	Расширенные параметры BSS и IBSS
Код страны [Country code ]	Код идентификатор страны для соблюдения регуляторных правил региона
Канальная информация	Канал, используемый ТД или IBSS
Карта индикации трафика [Traffic Indication Map (TIM)]	Поле, используемое во время процесса сбережения энергии
Загрузка BSS [BSS Load]	Поле, определенное 802.11e, которое является хорошим показателем загрузки канала
Возможности QoS	Информация о Качестве сервиса и Расширенном Распределенном Доступе к Каналу(EDCA)
Возможности Надежной Безопасной Сети [Robust Security Network (RSN) capabilities]	Информация о шифре TKIP, CCMP, или GCMP и способе аутентификации
Возможности HT и VHT [HT and VHT capabilities]	Возможности 802.11n и 802.11ac
Возможности HE [HE capabilities]	Возможности 802.11ax
Собственная информация производителя	Уникальная или специфичная для производителя информация

Кадры маяки [beacon frame] содержат всю необходимую информацию для того, чтобы клиентская станция узнала о параметрах базового состава сервиса до присоединения к BSS. Маяки передаются в заданное время каждые 102,4 миллисекунды, что означает, что ТД передает маяк около 10 раз в секунду. Этот интервал можно настроить на ТД, но его невозможно выключить. Некоторые руководства по проектированию БЛВС рекомендуют увеличивать *интервал маяка [beacon interval]* как средство уменьшения накладных расходов [overhead]. В большинстве случаев, увеличение интервала маяка – это очень плохая идея, потому что это может негативно ударить по подключению клиентов. ТД использует кадры маяки для информирования клиентских станций обо всех настроенных возможностях любого BSS, который поддерживает ТД.

Если ТД настроена для нескольких SSID, ТД будет передавать кадры маяки для каждого SSID. Последствия накладных расходов [overhead] при передаче нескольких маяков будут обсуждаться более детально в Главе 13 “Концепции Проектирования БЛВС”.

## УПРАЖНЕНИЕ 9.1

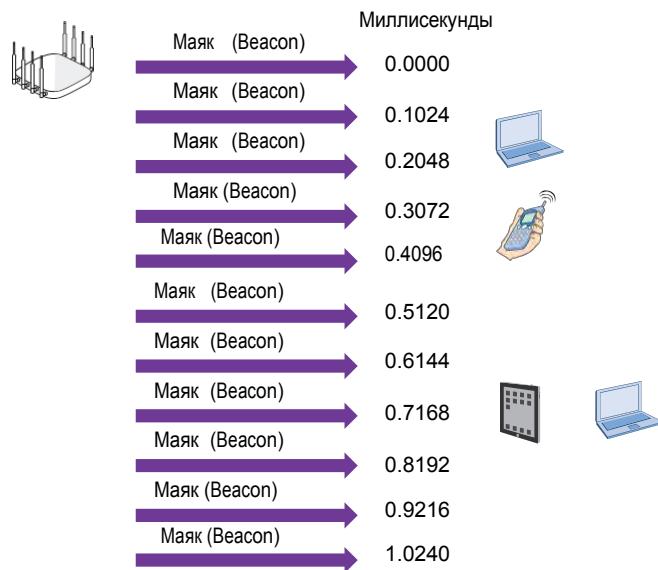
### Просмотр Кадров-Маяков

- Чтобы выполнить это упражнение, вам нужно сначала скачать файл CWNA-CH9.PCAPNG с онлайн ресурса этой книги, который может быть доступен по адресу [www.wiley.com/go/cwnasg6e](http://www.wiley.com/go/cwnasg6e).
- После загрузки файла, вам понадобится программное обеспечение по анализу пакетов. Если у вас на компьютере еще не установлен анализатор пакетов, вы можете загрузить Wireshark с [www.wireshark.org](http://www.wireshark.org).
- Используя анализатор пакетов, откройте файл CWNA-CH9.PCAPNG. Большинство анализаторов пакетов показывают список перехваченных кадров в верхнем разделе экрана, с последовательно пронумерованным каждым кадром в первой колонке.
- Кликните по одному из первых 10 кадров. Все эти кадры являются кадрами маяками (beacon frame).
- После выбора одного кадра маяка, в нижнем разделе экрана, пробегитесь по информации, находящейся внутри тела кадра-маяка. Разверните комментарии к пакету (Packet comments) для получения дальнейших указаний по просмотру кадра-маяка. Вы можете развернуть раздел путем нажатия на знак плюса (или знака больше) около раздела.

## Пассивное сканирование

Для того, чтобы станция была способна подключиться к ТД, он должна сначала обнаружить ТД. Станция обнаруживает ТД или слушая, чтобы услышать ТД (пассивное сканирование [passive scanning]), или осуществляя поиск ТД (активное сканирование [active scanning]). Клиентская станция находится в состоянии 1 машины состояний 802.11 во время этих фаз обнаружения. При пассивном сканировании, клиентская станция слушает, чтобы услышать кадры маяки, которые непрерывно посыпаются точкой доступа, как показано на Рисунке 9.17. Как упоминалось ранее, маяки посыпаются в заданное время каждые 102,4 миллисекунды. В перегруженных средах БЛВС точное время передачи будет слегка варьироваться из-за борьбы за среду всех станций в BSS, включая ТД.

**РИСУНОК 9.17** Пассивное сканирование



Клиентская станция будет слушать, чтобы услышать маяк, который содержит тот же самый SSID, который был преднастроен в программном обеспечении клиентской станции. Пассивное сканирование предоставляет начальное средство клиенту, чтобы узнать все возможности BSS, которые поддерживает ТД. Когда станция слышит маяк, она может попытаться подключиться к этой БЛВС, используя последующие карты управления. Если клиентская станция слышит маяки от нескольких ТД с одним и тем же SSID, она определит, какая ТД имеет лучший сигнал, и попытается подключиться к этой ТД.

Также, станции могут использовать один или оба метода сканирования для обнаружения существующих БЛВС. Когда развернут независимый базовый состав сервиса (IBSS), то все станции в режиме "на лету" [ad hoc] по очереди передают маяки [beacons], так как нет ТД. Пассивное сканирование в среде "на лету" [ad hoc] происходит также как это происходит в базовом составе сервиса (BSS).

## Активное Сканирование

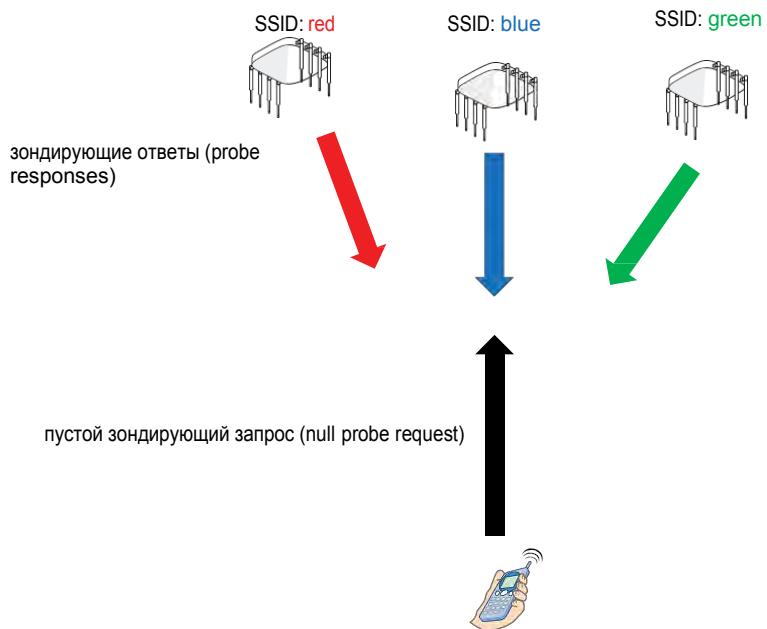
Обнаружение БЛВС путем сканирования всех возможных каналов и прослушивания маяков является неэффективным методом для клиента, чтобы найти все ТД на всех каналах. Чтобы улучшить этот процесс обнаружения, клиентские станции также используют, что называется, *активное сканирование [active scanning]*. В дополнение к пассивному сканированию ТД, клиентские станции активно сканируют их. При активном сканировании, клиентская станция передает кадр управления, который называется *зондирующий запрос [probe requests]*. Кадр зондирующего запроса также содержит информацию о возможностях клиентской станции, которой на начальном этапе можно поделиться с ТД. Некоторая клиентская информация, находящаяся в кадре зондирующего запроса, включает поддерживающие скорости передачи данных, возможности HT/VHT/HE, параметры SSID и другое.

Эти зондирующие запросы могут содержать SSID определенной БЛВС, которую ищет клиентская станция, или может искать любой SSID. Клиентская станция, которая ищет любой доступный SSID, посыпает зондирующий запрос [probe request] с полем SSID установленным в null (то есть в пустое значение). Другими словами - поле SSID не содержит никакого значения). Зондирующий запрос с конкретной информацией SSID, называется *направленный зондирующий запрос [directed probe request]*. Зондирующий запрос без информации о SSID называется *пустым зондирующим запросом [null probe request]*. По-русски, он, иногда, называется *нулевым зондирующим запросом*, однако такое название может ввести в заблуждение новичков в БЛВС, так как если зондирующий запрос содержит SSID со значением 0, он тоже может называться нулевым зондирующим запросом. Другой термин, иногда используемый для пустых зондирующих запросов – это wildcard SSID (шаблон всех SSID).

Если отправлен направленный зондирующий запрос, то все ТД, которые поддерживают этот конкретный SSID, и которые слышат этот запрос, должны ответить путем отправки зондирующего ответа [probe response]. Информация, которая содержится в теле кадра зондирующего ответа та же самая информация, которая находится в кадре маяка, за исключением карты индикации трафика [traffic indication map (TIM)]. Также как кадр маяка, кадр зондирующего ответа [probe response frame] содержит всю необходимую информацию, чтобы клиентская станция узнала о параметрах базового состава сервиса до присоединения к BSS.

Если отправлен пустой зондирующий запрос [null probe request], все ТД, которые слышат запрос, ответят путем отправки зондирующего ответа. Как показано на Рисунке 9.18, клиенты отправляют пустой зондирующий запрос на канале 36, и все три ТД с тремя разными SSID отвечают.

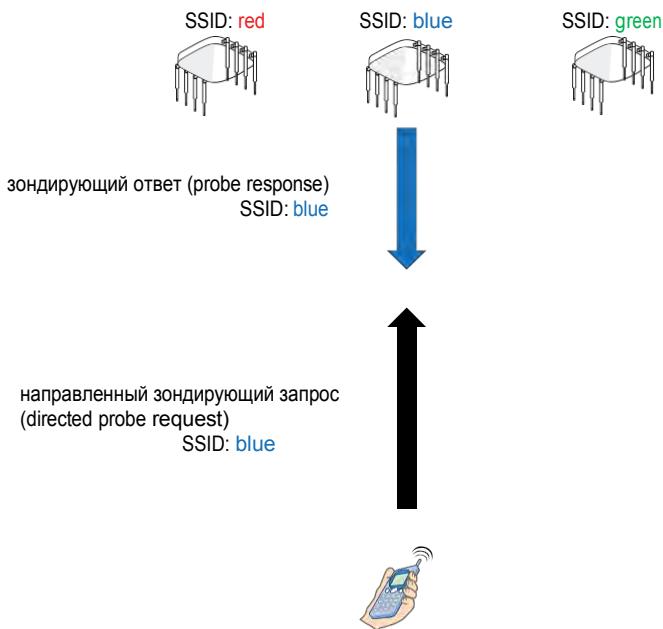
**Р И С У Н О К 9.18** Активное сканирование – пустые зондирующие запросы [null probe requests]



Если отправлен направленный зондирующий запрос, то ответят только ТД, настроенные с

таким же SSID. Как представлено на Рисунке 9.19, клиент отправляет направленные зондирующие запросы с SSID blue, и единственная ТД, которая отвечает – это ТД, которая также поддерживает SSID blue.

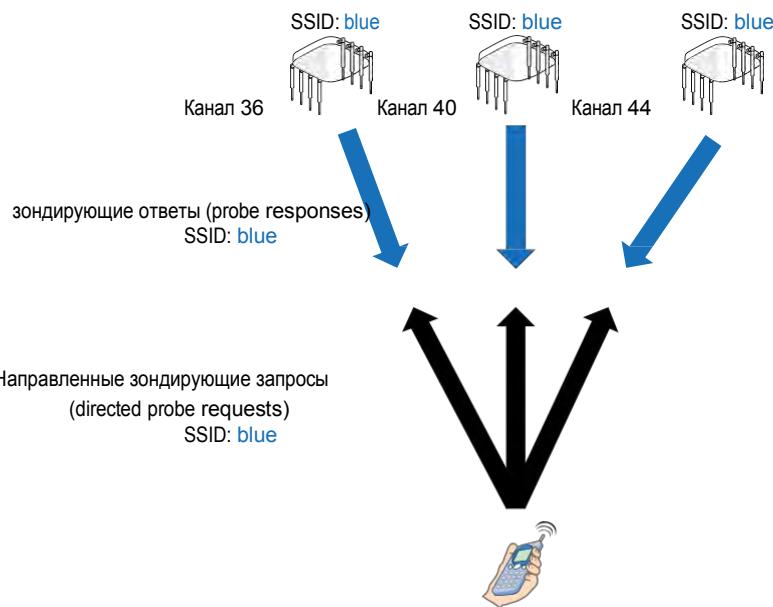
**Р И С У Н О К 9 . 1 9** Активное сканирование—направленный зондирующий запрос (directed probe request)



Один недостаток пассивного сканирования – это то, что кадры управления-маяки рассылаются всем только на том же канале, на котором вещает ТД. Наоборот, активное сканирование использует кадры зондирующих запросов, которые отправляются по всем каналам, доступным клиентской станции. Если клиентской станции получает зондирующие ответы от нескольких ТД, то клиентской станцией используются характеристики силы сигнала и качества, чтобы определить какая ТД имеет самый лучший сигнал, и таким образом подключиться к ней. Как показано на Рисунке 9.20, клиентская станция последовательно посылает зондирующие запросы на каждом поддерживаемом канале. По факту, для клиентской станции, которая уже ассоциирована с ТД и передающая данные, является обычным делом выходить за канал и продолжать рассыпать зондирующие запросы каждые несколько секунд по другим каналам. Основное назначение внеканального зондирования [off-channel probing] – это то, что клиентская станция может найти другие ТД для потенциального переключения(роуминга) на них. Путем непрерывного активного сканирования и рассылки зондирующих запросов по нескольким каналам, клиентская станция может поддерживать и обновлять список известных ТД. Если клиентской станции нужно переключиться, она обычно может сделать это быстрее и более эффективно.

Как часто клиентская станция уходит с канала для активного сканирования является проприетарным, и зависит от драйверов клиентского устройства. Например, радиомодули 802.11 в мобильных устройствах, таких как смартфон или планшет, вероятно, будут рассыпать зондирующие запросы по всем каналам более часто, чем радиомодули 802.11 в ноутбуках. Некоторые клиентские устройства имеют способность подстраивать скорость зондирования (скорость рассылки зондирующих запросов). Выполняя Упражнение 9.2, вы сможете посмотреть в кадры зондирующего запроса и зондирующего ответа.

**Р И С У Н О К 9 . 2 0**      Зондирующие запросы—несколько каналов



**У П Р А Ж Н Е И Е 9 . 2**

**Осмысление Зондирующих Запросов и Ответов**

- Чтобы выполнить это упражнение, вам понадобится сначала скачать файл CWNA-CH9.PCAPNG с онлайн ресурса этой книги, который доступен по адресу [www.wiley.com/go/cwnasgbe](http://www.wiley.com/go/cwnasgbe).
- После загрузки файла, вам понадобится программное обеспечение по анализу пакетов, чтобы открыть файл. Если у вас на компьютере еще не установлен анализатор пакетов, вы можете скачать Wireshark с [www.wireshark.org](http://www.wireshark.org).
- Используя анализатор пакетов, откройте файл CWNA-CH9.PCAPNG. Большинство анализаторов пакетов показывают список собранных пакетов в верхнем разделе экрана, с последовательно пронумерованными кадрами в первой колонке.
- Прокрутите вниз список кадров и щёлкните кадр #13684, который является зондирующим запросом [probe request].
- В нижнем разделе экрана, посмотрите на поле SSID в теле кадра, и обратите внимание, что это направленный зондирующий запрос. Раскройте комментарии пакета (Packet comments) для дальнейших указаний по просмотру зондирующего запроса.
- Кликните кадр #13685, который является зондирующим ответом [probe response].

7. В нижней части экрана, пробегитесь по информации, находящейся внутри тела кадра, и заметьте, что информация аналогична кадру маяку. Раскройте комментарии к пакету (Packet comments) для дальнейшего указания по просмотру зондирующего ответа.
  8. Щёлкните по кадру #429, который является зондирующим запросом [probe request]. Посмотрите на поле SSID в теле кадра, и заметьте, что это пустой зондирующий запрос [null probe request], так как он не содержит значение SSID. Разверните комментарии к пакету (Packet comments) для дальнейших указаний по просмотру пустого зондирующего запроса.
  9. Кликните кадры #430, #432, #434, #436, and #438. Заметьте, что это пять зондирующих ответов на пустой зондирующий запрос [null probe request]. Каждый зондирующий ответ имеет разный SSID. Разверните комментарии к пакету(Packet comments) для получения дальнейших указаний по просмотру разных зондирующих ответов.
- 

## Аутентификация

*Аутентификация [Authentication]* является первой из двух шагов, требующихся для подключения к базовому составу сервиса 802.11. И аутентификация и ассоциация должны происходить, в таком порядке, прежде чем клиент 802.11 может передать трафик через ТД другому устройству в сети.

Аутентификация является процессом, который часто неправильно понимается. Когда много людей думают об аутентификации, они думают о, что в общем называется, сетевой аутентификацией – вводом имени пользователя и пароля для того, чтобы получить доступ к сети. В этой главе, мы говорим об аутентификации 802.11. Когда устройству 802.3 нужно связаться с другими устройствами, первый шаг – это воткнуть Ethernet кабель в Ethernet розетку. Когда этот кабель воткнут, клиент создает физический канал связи к проводному коммутатору, и теперь может начинать передачу кадров. Когда устройству 802.11 нужно связаться, оно должно сначала аутентифицироваться с ТД, или с другими станциями, если они настроены в режим "на лету" [ad hoc]. Эта аутентификация намного большая задача, чем подключение Ethernet кабеля в розетку. Аутентификация 802.11 только устанавливает начальное соединение между клиентом и ТД. Думайте об этом как о подтверждении того, что оба устройства являются действительными устройствами 802.11.

Раз клиентская станция обнаружила ТД активным или пассивным сканированием, клиентская станция использует аутентификационные кадры управления 802.11, чтобы перейти к состоянию 2 машины состояний 802.11.

Первоначальный стандарт 802.11 определял два метода аутентификации: аутентификация Открытой Системы [Open System authentication] и аутентификация с Общим Ключом [Shared Key authentication]. Аутентификация с Общим Ключом использует Проводной Эквивалент Секретности [Wired Equivalent Privacy (WEP)], чтобы аутентифицировать клиентские станции, и требует, чтобы статический ключ WEP был настроен и на станции и на точке доступа. Так как WEP это устаревший метод безопасности, аутентификация с Общим Ключом просто больше не используется. Аутентификация с общим ключом кратко описана в Главе 17 “Архитектура Сетевой безопасности 802.11”.

## Аутентификация Открытой Системы

*Аутентификация Открытой Системы [Open System authentication]* обеспечивает аутентификацию без проведения какого-либо типа верификации (подтверждения) клиента.

Фактически это обмен приветствиями [hellos] между клиентом и ТД. Это считается пустой или нулевой аутентификацией [null authentication], потому что никакого обмена или подтверждения личности не происходит между устройствами. Аутентификация Открытой Системы осуществляется с обменом кадрами между клиентом и ТД, как показано в Упражнении 9.3. После того, как клиентская станция обменялась аутентификационными кадрами управления с ТД, клиент переходит в состояние 2 машины состояний 802.11.

Из-за своей простоты, аутентификация Открытой Системы [Open System authentication] также используется совместно с более продвинутыми методами безопасной сетевой аутентификации, таким как аутентификация PSK и 802.1X/EAP.

### УПРАЖНЕНИЕ 9.3

#### Использование Аутентификации Открытой Системы

- Чтобы выполнить это упражнение, вам нужно сначала скачать файл CWNA-CH9.PCAPNG с онлайн ресурса книги, который может быть доступен по адресу [www.wiley.com/go/cwnasg6e](http://www.wiley.com/go/cwnasg6e).
- После того, как файл загружен, вам нужно программное обеспечение по анализу пакетов. Если у вас на компьютере еще не установлен анализатор сетевых пакетов, вы можете загрузить Wireshark по адресу [www.wireshark.org](http://www.wireshark.org).
- Используя анализатор пакетов, откройте файл CWNA-CH9.PCAPNG. Большинство анализаторов пакетов показывают список собранных кадров в верхнем разделе экрана, с последовательно пронумерованными кадрами в первом столбце.
- Прокрутите вниз список кадров и кликните по кадру #871, который является аутентификационным запросом [authentication request]. Разверните комментарии к пакету [Packet comments] для дальнейших указаний по просмотру аутентификационного кадра.
- В нижнем разделе экрана, посмотрите на MAC заголовок 802.11 и посмотрите на адрес источника [source address] и адрес назначения [destination address].
- Щелкните кадр #873, который является аутентификационным ответом [authentication response]. Разверните комментарии к пакету (Packet comments) для дальнейших инструкций по просмотру кадра аутентификации.
- Посмотрите на MAC заголовок 802.11 и посмотрите, что адрес источника – это BSSID точки доступа, а адрес назначения – это MAC адрес клиента, который послал запрос на аутентификацию [authentication request]. Посмотрите в тело кадра, и обратите внимание, что аутентификация была успешна.

## Ассоциация

После того, как станция аутентифицировалась с ТД, следующий шаг – ассоциироваться с ТД. Когда клиентская станция ассоциируется, она становится членом базового состава сервиса [basic service set (BSS)]. *Ассоциация [Association]* означает, что клиентская станция установила соединение 2ого уровня с ТД и присоединилась к BSS. Клиентская станция посыпает к ТД кадр управления – запрос на ассоциацию [association request], ожидая разрешение на присоединение к BSS. ТД посыпает кадр управления – ответ на ассоциацию [association response] клиенту, или предоставляя или отказывая в разрешении на присоединение к BSS.

Эти кадры используются клиентской станцией для перехода в состояние 3 машины состояний 802.11. В теле кадра ответа на ассоциацию [association response] находится идентификатор ассоциации [association identifier (AID)], уникальный номер ассоциации, выдаваемый каждому ассоциированному клиенту. Вы узнаете позже в этой главе, что AID используется во время управления электропитанием. В Упражнении 9.4 вы увидите, что кадры запроса и ответ на ассоциацию также используются как финальные уведомления о возможностях между ТД и клиентской станцией.

## УПРАЖНЕНИЕ 9.4

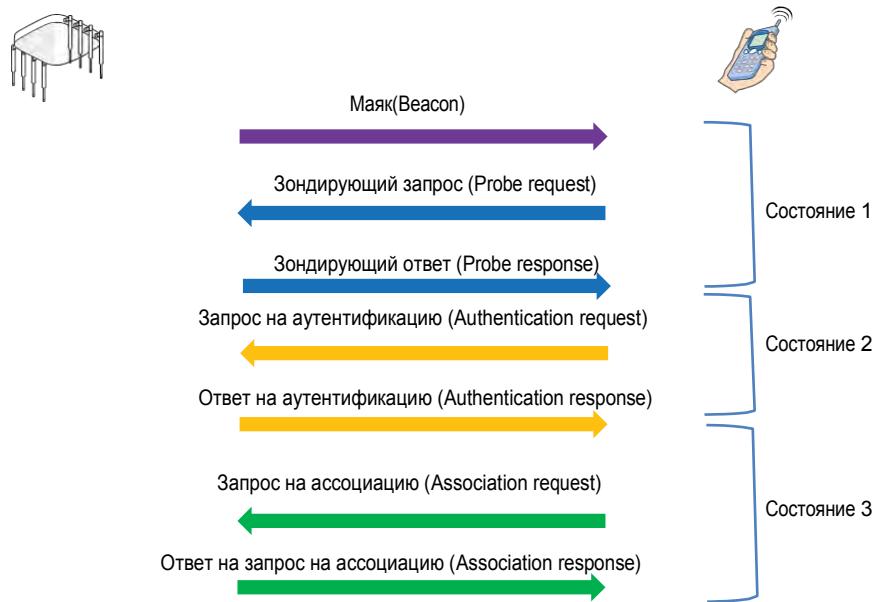
### Понимание Ассоциации

- Чтобы выполнить это упражнение, вам нужно сначала скачать файл CWNA-CH9.PCAPNG с онлайн ресурса книги, который может быть доступен по адресу [www.wiley.com/go/cwnasg6e](http://www.wiley.com/go/cwnasg6e).
- После загрузки файла, вам нужна программа по анализу сетевых пакетов, чтобы открыть файл. Если на вашем компьютере еще не установлен анализатор пакетов, вы можете скачать Wireshark с [www.wireshark.org](http://www.wireshark.org).
- Используя анализатор пакетов, откройте файл CWNA-CH9.PCAPNG. Большинство анализаторов пакетов показывают список собранных кадров в верхнем разделе экрана, с последовательно пронумерованными кадрами в первом столбце.
- Прокрутите ниже список кадров, и кликните кадр #875, который является запросом на ассоциацию [association request]. Посмотрите на тело кадра. Разверните комментарии к пакету для дальнейших указаний по просмотру кадра запроса на ассоциацию.
- Щелкните кадр #877, который является ответом на запрос на ассоциацию [association response]. Посмотрите на тело кадра и заметьте, что ассоциация была успешна, и клиент получил номер AID. Разверните комментарии к пакету для дальнейших указаний к просмотру кадра ответа на ассоциацию.

Если никакая RSN безопасность не используется, то, когда клиентская станция завершила ассоциацию, устройство достигает состояния 3 машины состояний 802.11 и присоединено к BSS. В этой точке, клиентская станция может двинуться за пределы уровня 2, запросить IP адрес, и начать связываться на верхних уровнях. Рисунок 9.21 иллюстрирует все обмены кадров, необходимых между клиентской станцией и ТД, чтобы клиентская станция достигла состояния 3 и присоединилась к BSS.

Что насчет состояния 4 машины состояний 802.11? Если аутентификация PSK или 802.1X/EAP настроена на ТД, то клиентская станция все еще не присоединена к BSS. Клиент ассоциирован, однако, находится в ожидании RSN аутентификации. Если используется PSK аутентификация, то клиент и ТД должны иметь совпадающий WPA2 пароль [passphrase]. Также, еще один обмен кадров, называемый 4x Сторонним Рукопожатием [4-Way Handshake], должен пройти, чтобы создать динамические ключи шифрования для обоих радиомодулей.

РИСУНОК 9.21 Присоединение к BSS



Если используется аутентификация 802.1X/EAP, то будет обмен серии кадров аутентификации EAP между клиентом и RADIUS сервером для подтверждения клиентских параметров безопасности. Также будет происходить обмен 4x Стороннего Рукопожатия [4-Way Handshake] после 802.1X/EAP, чтобы создать динамические ключи шифрования для обоих радиомодулей.

После завершения любого метода RSN аутентификации, и после того, как обмен 4x Стороннего Рукопожатия [4-Way Handshake] создал ключи шифрования, клиентская станция достигает состояния 4 машины состояний 802.11 и становится членом BSS. В этой точке, клиентская станция может двигаться далее 2ого уровня, запросить IP адрес, и начать взаимодействие на верхних уровнях. Детальное объяснение 4x Стороннего Рукопожатия [4-Way Handshake] можно найти в Главе 17.

## Базовая и Поддерживаемые Скорости Передачи

Как вы узнали из глав ранее, стандарт 802.11-2020 определяет поддерживаемые скорости для различных радиотехнологий. Например, радиомодули HR-DSSS (802.11b) способны поддерживать скорости передачи данных 1, 2, 5.5, и 11 Мбит/с.

Радиомодули ERP (802.11g) способны поддерживать скорости передачи данных HR-DSSS, а также способны поддерживать скорости передачи ERP-OFDM: 6, 9, 12, 18, 24, 36, 48, и 54 Мбит/с.

Определенные скорости передачи данных могут быть настроены на любой ТД как *требуемые скорости передачи данных [required rates]*. Стандарт 802.11-2020 определяет требуемые скорости передачи данных как *базовые скорости передачи данных [basic rates]*. Нужно понимать, что ТД будет передавать все кадры управления на самой низкой настроенной базовой скорости передачи данных. Кадры данных могут быть переданы на существенно большей скорости передачи данных.

Для того, чтобы клиентская станция успешно ассоциировалась с ТД, станция должна быть способна работать с использованием настроенных базовых скоростей передачи

данных, которые требует ТД. Если клиентская станция не способна работать на всех базовых скоростях передачи данных, клиентская станция не сможет стать ассоциированной с ТД, и ей не будет разрешено присоединиться к BSS.

В дополнение к базовым скоростям передачи данных, ТД определяет набор поддерживаемых скоростей. Этот набор поддерживаемых скоростей передачи данных сообщается ТД в кадре-маяке, а также в некоторых других кадрах управления.

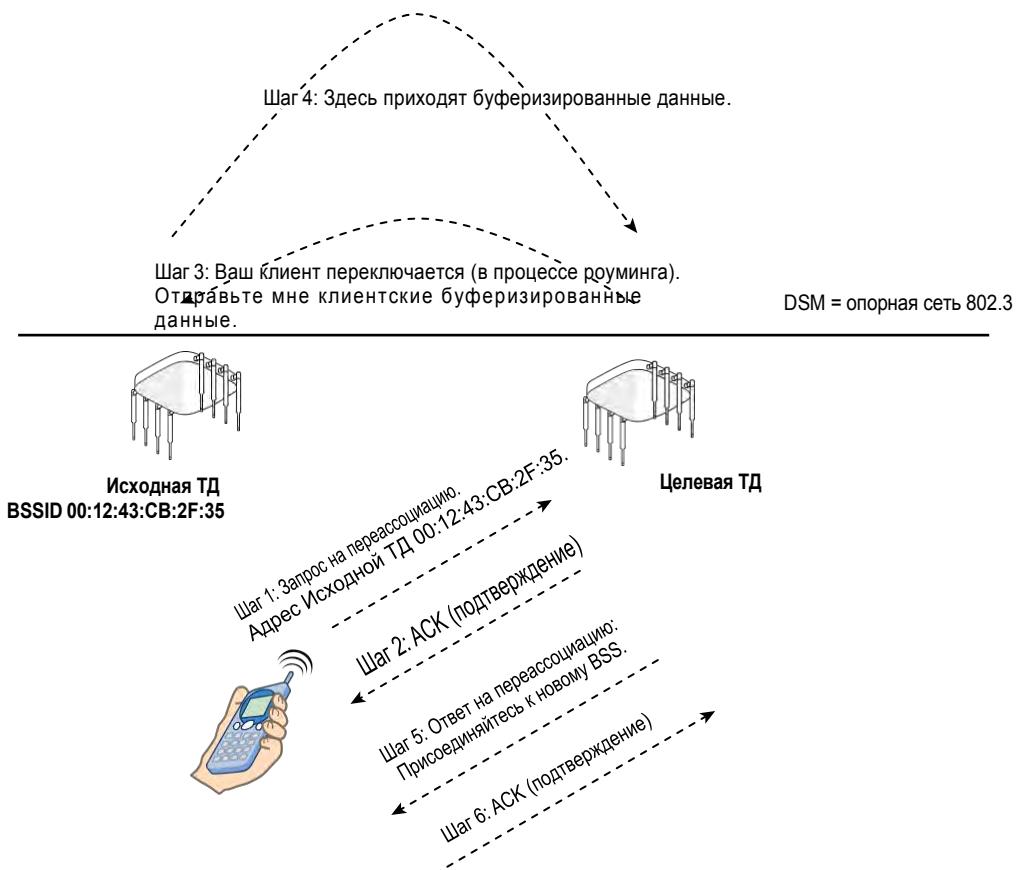
Поддерживаемые скорости являются скоростями передачи данных, которые ТД предлагает клиентской станции, но клиентская станция не обязана поддерживать все из них.

## Переассоциация

Когда клиентская станция решает переключиться на новую ТД, она посыпает кадр запроса на *переассоциацию [reassociation]* новой ТД. Кадры переассоциации используются клиентской станцией для перехода с исходного BSS на новый BSS. Кадр переассоциации – это фактически роуминговый запрос, посыпаемый от клиентской станции к целевой ТД. Переассоциация происходит после того, как клиент и ТД пройдут через следующие шаги:

- На первом шаге, клиентская станция отправляет кадр запроса на переассоциацию новой ТД. Как показано на Рисунке 9.22, кадр запроса на переассоциацию включает BSSID (MAC address) радиомодуля ТД, с которой он на текущий момент соединен. (Мы будем называть ее как исходная ТД [original AP]).

**Р И С У Н О К 9 . 2 2**      Процесс переассоциации



2. Затем новая ТД отвечает станции подтверждением (ACK).
3. Новая ТД пытается связаться с исходной ТД через среду системы распространения [distribution system medium (DSM)].

Новая ТД пытается уведомить исходную ТД о переключении(роуминге) клиента, и запрашивает, чтобы исходная ТД переслала все буферизированные данные. Помните, что любое общение между ТД через DSM не определено стандартом 802.11-2020, и является собственной разработкой производителя. В решения БЛВС на основе контроллера, обмен данными между ТД может происходить внутри контроллера. В безконтроллерной архитектуре, ТД будут общаться друг с другом на границе [edge] сети.

4. Если это общение между ТД успешно, то исходная ТД будет использовать среду системы распространения для пересылки любых буферизированных данных к новой ТД.
5. Новая ТД отправляет кадр ответа на переассоциацию переключающемуся клиенту по беспроводной среде.
6. Клиент отправляет подтверждение (ACK) новой ТД, подтверждая, что он получил ответ на переассоциацию, и намеревается переключиться. В большинстве случаев, имеет место быть безопасность WPA2, и тогда будет еще один финальный шаг, который не показан на Рисунке 9.22. Клиент и целевая ТД продолжат обмен кадров с 4x Сторонним Рукопожатием, чтобы сгенерировать уникальные ключи шифрования между двумя радиомодулями.

Если переассоциация оказалась не удачной, клиент сохраняет свое соединение с исходной ТД, и или продолжает работать с ней, или пытается переключиться на другую ТД. В Упражнении 9.5, вы можете посмотреть на кадры запроса и ответа на переассоциацию.

## УПРАЖНЕНИЕ 9.5

### Понимание Переассоциации

1. Чтобы выполнить это упражнение, вам нужно сначала скачать файл CWNA-CH9.PCAPNG с онлайн ресурса книги, который доступен по адресу [www.wiley.com/go/cwnasg6e](http://www.wiley.com/go/cwnasg6e).
2. После того как файл загружен, вам нужен программный анализатор пакетов, чтобы открыть файл. Если на вашем компьютере еще не установлен анализатор пакетов, вы можете загрузить Wireshark (произносится как Уайешак, переводится как Проводная Акула) с [www.wireshark.org](http://www.wireshark.org)
3. Используя анализатор пакетов, откройте файл CWNA-CH9.PCAPNG. Большинство анализаторов пакетов показывают список собранных файлов в верхнем разделе экрана с последовательно пронумерованными кадрами в первой колонке.
4. Прокрутите список кадров вниз и кликните по кадру #7626, который является запросом на переассоциацию [reassociation request]. Посмотрите на тело кадра и заметьте адрес текущей ТД. Разверните комментарии к пакету (Packet comments) для дальнейших указаний по просмотру кадра запроса на переассоциацию.
5. Щелкните кадр #7628, который является ответом на переассоциацию. Посмотрите на тело кадра и обратите внимание, что переассоциация была успешной, и затем клиент получил номер AID. Разверните комментарии к пакету (Packet comments) для дальнейших указаний по просмотру кадра ответа на переассоциацию [reassociation response].

## Деассоциация

*Деассоциация [Disassociation]* - это уведомление, а не запрос. Если станция хочет деассоциироваться [отключиться] от ТД, или ТД хочет деассоциироваться от станции, любое из устройств может отправить кадр деассоциации [disassociation frame]. Это мягкий способ завершения ассоциации. Клиент поступает так, когда вы выключаете операционную систему. ТД может делать так, если она отключается от сети для обслуживания. Кадр деассоциации, отправленный ТД, отправляет клиентов из состояния 3 или 4 назад в состояние 2 машины состояний 802.11. Каждый кадр деассоциации несет код причины почему происходит деассоциация. Например, ТД может послать кадр деассоциации с кодом причины 4 клиенту, который неактивен. Все возможные коды причин могут быть найдены в разделе 9.4.17 стандарта 802.11-2020.

## Деаутентификация

Также как и деассоциация, кадр *деаутентификации [deauthentication]* является уведомлением [notification], а не запросом. Если станция хочет деаутентифицироваться от ТД, или ТД хочет деаутентифицироваться от станций, каждое устройство может отправить кадр деаутентификации. Так как аутентификация является предварительным условием для ассоциации, кадр деаутентификации автоматически вызовет деассоциацию. Кадр деаутентификации, отправленный ТД, отправляет клиента из состояний 2,3 или 4 обратно в состояние 1 машины состояний 802.11. Кадры деаутентификации фактически заставляют клиентскую станцию начать заново искать и присоединиться к BSS. Каждый кадр деаутентификации несет код причины почему происходит деаутентификация. Например, ТД может отправить кадр деаутентификации с кодом причины 23 клиенту, который не прошел аутентификацию 802.1X/EAP, и возвращает клиента обратно в состояние 1. Все возможные коды причин можно найти в разделе 9.4.17 стандарта 802.11-2020.

## Кадр Действия

Кадр *действия [action frame]* является типом кадра управления, используемого в качестве триггера для запуска определенных действий в BSS. Кадры действия могут быть отправлены точками доступа или клиентскими станциями. Кадр действия предоставляет информацию и направление что нужно сделать. Кадры действия были впервые представлены в 802.11h, так как подтип для кадров управления был исчерпан. Кадр действия иногда называется, как “кадр управления, который все может сделать”. По мере появления новых технологий 802.11, появилась необходимость в новых кадрах управления для переноса информации и запуска определенных действий. Вместо создания новых кадров управления, кадры действия могут выполнить эту работу. Рисунок 9.23 показывает структуру кадра действия.

**Р И С У Н О К 9 . 2 3** Структура кадра действия



Тело кадра действия содержит следующие три раздела:

- Категория: Описывает тип кадра действия. Категория позволяет вам узнать, к какой семье принадлежит кадр действия, и какой протокол представляет ее.
- Действие: Действие, которое нужно сделать. Обычно это номер. Вам нужно знать категорию, чтобы понять какое действие вызывается. На текущий момент существует 30 значений различных категорий.
- Элементы: Добавляют дополнительную информацию, касающуюся действия.

Полный список всех текущих кадров действия можно найти в разделе 9.6 стандарта 802.11-2020. На текущий момент существует около 30 различных типов кадров действия. Один пример того, как кадры действия используются – это *оповещение о смене канала [channel switch announcement (CSA)]* от ТД, передающей на канале с *динамическим выбором частоты [dynamic frequency selection (DFS)]*. Если обнаружен радар на текущей DFS частоте, то ТД информирует все ассоциированные клиентские станции о необходимости переместиться на другой канал. Кадры действия также используются в качестве кадров запроса и отчета по *контролю мощности передачи [transmit power control (TPC)]*. ТД может сказать ассоциированным клиентским станциям, что она поддерживает еще TPC, чтобы те настроили свои уровни мощности по передаче, чтобы соответствовать уровням мощности ТД. Глубокое обсуждение каналов DFS и механизмов TPC можно найти в Главе 13.

Еще один пример кадра действия – это запросы и ответы об отчете о соседях [*neighbor report*], который могут использовать 802.11k-совместимые радиомодули. Как показано на Рисунке 9.6, клиентские станции используют информацию отчетов о соседях, чтобы получить информацию от ассоциированной ТД о потенциальных соседях для переключения(роуминга). Как определено поправкой 802.11k-2008, информация отчета о соседях помогает процессу быстрого роуминга предоставляя клиенту метод для запроса ассоциированной ТД измерить и сообщить о соседних ТД, доступных внутри одного и того же мобильного домена. Это может ускорить процесс сканирования клиентом, путем информирования клиентского устройства о ближайших ТД, на которые он может переключиться. Информация отчета о соседях обычно доставляется через обмен кадров запрос/ответ внутри кадров действия 802.11.

## УПРАЖНЕНИЕ 9.6

### Обзор Кадров Действия

1. Чтобы выполнить это упражнение, вам нужно сначала загрузить файл ACTION.PCAPNG с онлайн ресурса книги, который доступен по адресу [www.wiley.com/go/cwnasg6e](http://www.wiley.com/go/cwnasg6e).
2. После загрузки файла, вам нужен программный анализатор пакетов, чтобы открыть файл. Если на вашем компьютере еще не установлен анализатор пакетов, вы можете скачать Wireshark с [www.wireshark.org](http://www.wireshark.org).
3. Используя анализатор пакетов, откройте файл ACTION.PCAPNG. Большинство анализаторов пакетов отображают список собранных кадров в верхнем разделе экрана с последовательно пронумерованными кадрами в первом столбце. Разверните комментарии к пакету (Packet comments) для дальнейших указаний по просмотру кадров действия в пакетах #103 и #105.
4. Прокрутите вниз список кадров и кликните пакет #103, который является кадром действия 802.11, переданным клиентским устройством Apple iOS. Обычно, в нижнем разделе экрана находится окно с детализацией пакета. Этот раздел содержит

подробные комментарии о выбранном кадре. В этом окне, найдите и разверните кадр действия. В теле кадра действия разверните параметры с метками или тэгми [tagged parameters] и обратите внимание, что этот кадр действия используется в качестве запрос об отчете о соседях [neighbor report request]). Клиент спрашивает ТД – есть ли у ТД информация о каких-нибудь соседних ТД.

5. Щелкните пакет #105, который является кадром действия 802.11, переданным ТД. В теле кадра действия, разверните фиксированные параметры [fixed parameters] и обратите внимание, что этот кадр действия используется в качестве ответа с отчетом о соседях [neighbor report response]. В теле кадра действия, разверните параметры с метками [tagged parameters] и посмотрите отчет о соседях [neighbor report] о ТД с BSSID 08:ea:44:76:b5:68, которая передает на канале 48.
-

# Кадры Контроля

Кадры контроля 802.11 [*802.11 control frames*] помогают с доставкой кадров данных, и передаются с одной из базовых скоростей. Контрольные кадры также используются для очистки канала, занятия канала, и поддержки односторонних [unicast] подтверждений кадров. Как ранее упоминалось, контрольные кадры имеют только MAC заголовок и окончание; у них нет тела кадра. Информация, находящаяся в MAC заголовке, является достаточной для выполнения задач, определенных для контрольных кадров 802.11.

Далее представлен список всех 12 подтипов контрольных кадров, определенных на текущий момент стандартом 802.11-2020:

- |                                |                                      |
|--------------------------------|--------------------------------------|
| ▪ TACK (TWT acknowledgment)    | Подтверждение TWT                    |
| ▪ Beamforming report poll      | Опрос отчета о/для формирования луча |
| ▪ VHT NDP announcement         | Оповещение VHT NDP                   |
| ▪ Control frame extension      | Расширение контрольного кадра        |
| ▪ Control wrapper              | Контрольная обертка                  |
| ▪ Block ACK request (BAR)      | Запрос на Блоковое подтверждение     |
| ▪ Block ACK (BlockAck)         | Блоковое подтверждение               |
| ▪ Power save-poll (PS-Poll)    | Опрос по сбережению электропитания   |
| ▪ Request-to-send (RTS)        | Запрос на отправку                   |
| ▪ Clear-to-send (CTS)          | Чисто для отправки                   |
| ▪ Acknowledgment (ACK)         | Подтверждение                        |
| ▪ Contention Free-End (CF-End) | Конец отсутствия конкурентной борьбы |

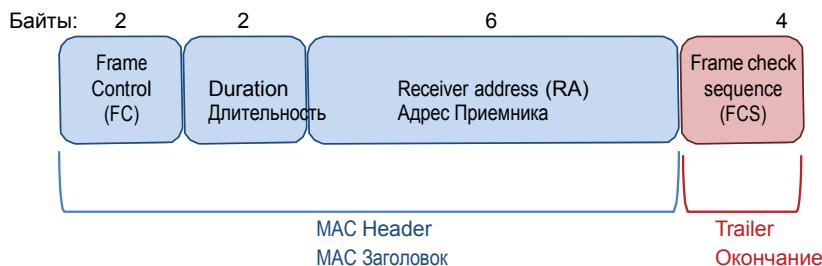
Теперь мы обсудим наиболее часто используемые контрольные кадры 802.11.

## Кадр подтверждения (ACK)

Кадр подтверждения [*ACK frame*] - это один из 12 контрольных кадров и один из ключевых компонентов метода контроля доступа к среде 802.11 CSMA/CA. Поскольку 802.11 является беспроводной средой, которая не может гарантировать успешную передачу данных, единственный способ для станции узнать, что кадр, который она передала, был правильно получен – это принимающей станции уведомить передающую станцию. Это уведомление выполняется с использованием ACK.

ACK – это просто кадр, состоящий из 14 октетов информации, как показано на Рисунке 9.24. Когда станция принимает однонаправленный [unicast] кадр, она ждет короткий период времени, называемый *короткое межкадровое пространство* [*short interframe space (SIFS)*]. Приемная станция копирует MAC адрес передающей станции из кадра данных, и помещает его в поле Адрес Приемника [Receiver Address (RA)] кадра ACK. Как вы увидите в Упражнении 9.7, принимающая станция затем отвечает, передавая ACK. Если все идет хорошо, станция, которая отправила однонаправленный кадр, получает ACK со своим MAC адресом в поле RA, и теперь знает, что кадр был получен и не был поврежден. Доставка каждого однонаправленного [unicast] кадра должна быть подтверждена; в противном случае должна иметь место повторная передача [retransmission]. Кадр ACK – очень важный контрольный кадр, потому что он используется для подтверждения доставки всех однонаправленных кадров 802.11. Если произошел конфликт (коллизия), или если любая часть кадра повреждена, то циклическая резервная проверка [cyclic redundancy check (CRC)] не пройдет, и принимающий радиомодуль 802.11 не вернет кадр ACK передающему радиомодулю 802.11.

**РИСУНОК 9.24** Контрольный кадр ACK



За каждым однонаправленным [unicast] кадром должен следовать кадр ACK. Если по какой-либо причине однонаправленный кадр поврежден, то 32 битный CRC, называемая кадровая проверочная последовательность [frame check sequence (FCS)] не пройдет, и приемная станция не отправит ACK. Если за однонаправленным кадром не идет ACK, то он повторно передается. За редким исключением, широковещательные [broadcast] и многонаправленные [multicast] кадры не требуют подтверждений [acknowledgment].

## УПРАЖНЕНИЕ 9.7

### Понимание Подтверждения

- Чтобы выполнить это упражнение, вам нужно сначала загрузить файл CWNA-CH9.PCAPNG с онлайн ресурса книги, который доступен по адресу [www.wiley.com/go/cwnasg6e](http://www.wiley.com/go/cwnasg6e).
- После того, как файл загружен, вам понадобится программное обеспечение – анализатор пакетов, чтобы открыть файл. Если на вашем компьютере еще не установлен анализатор пакетов, вы можете скачать Wireshark с [www.wireshark.org](http://www.wireshark.org).
- Используя анализатор пакетов, откройте файл CWNA-CH9.PCAPNG. Большинство

анализаторов пакетов показывают список перехваченных кадров в верхнем разделе экрана, с последовательно пронумерованными кадрами в первом столбце.

Разверните комментарии к пакету (*packet comments*) для дальнейших указаний по просмотру кадров в пакетах #29073 и #29074.

4. Прокрутите вниз список кадров и кликните кадр #29073, который является кадром данных.
  5. Кликните кадр #29074, который является кадром ACK (подтверждения).
  6. Рассмотрите обмен кадров между кадром #29073 и кадром #29088. Обратите внимание, что все односторонние [unicast] кадры подтверждены принимающей станцией.
-

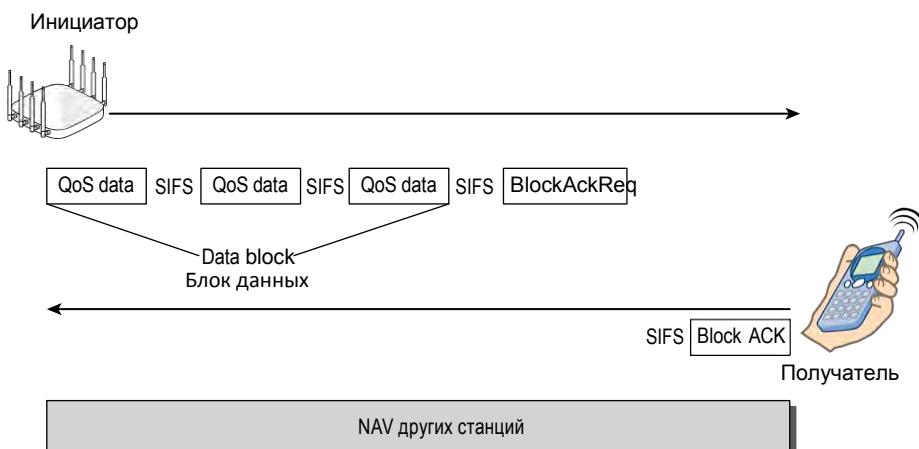
## Блоковое Подтверждение

Поправка 802.11e ввела механизм **Блокового подтверждения [Block acknowledgment (BA)]**, который теперь определен в стандарте 802.11-2020. Блоковое подтверждение [Block ACK] улучшает эффективность канала путем агрегации нескольких подтверждений в один единый кадр подтверждения. Существует два типа механизма Блоковых подтверждений [Block ACK]: немедленный [immediate] и отложенный [delayed].

- Немедленное Блоковое подтверждение [Immediate Block ACK] предназначено для использования с трафиком с низкой задержкой.
- Отложенное Блоковое подтверждение [Delayed Block ACK] является более подходящим для трафика терпимого к задержкам.

В рамках этой книги, мы обсудим только немедленное Блоковое подтверждение [immediate Block ACK]. Как изображено на Рисунке 9.25, станция-инициатор отправляет блок кадров данных с поддержкой качества сервиса (QoS) станции-получателю. Инициатор запрашивает подтверждение всех кадров данных с поддержкой качества сервиса (QoS), посылая кадр запроса Блокового подтверждения [Block ACK request (BAR)]. Вместо подтверждения каждого однокастового [unicast] кадра независимо, блок из всех кадров данных с поддержкой качества сервиса (QoS) подтверждается одним Блоковым Подтверждением [Block ACK]. Битовая карта в Блоковом подтверждении [Block ACK] используется, чтобы указать статус каждого полученного кадра данных. Если только один из кадров поврежден, только этот кадр нужно будет повторно передать. Использование Блокового подтверждения [Block ACK] вместо традиционного подтверждения (ACK) является более эффективным методом, который сокращает накладные расходы (или overhead) при борьбе за среду. Блоковые подтверждения [Block ACKs] были изначально определены для использования с «взрывом кадров», как показано на Рисунке 9.25. Однако, Блоковые подтверждения [Block ACKs] в основном используются с агрегацией кадров A-MPDU. За подробностями обращайтесь к Главе 10.

**РИСУНОК 9.25** Немедленное Блоковое Подтверждение (Immediate Block ACK)



## PS-Poll

Когда используется устаревшее управление электропитанием, кадр *PS-Poll* является контрольным кадром 802.11, который используется клиентскими станциями, чтобы запросить ТД, чтобы ТД отправила буферизированный трафик для клиентской станции. Клиенты, использующие устаревшее управление электропитанием, отправят кадр PS-Poll точке доступа, чтобы запросить, чтобы ТД отправила буферизированный односторонний кадр к станции. Внутри кадра PS-Poll, поле Duration/ID используется в качестве значения идентификатора ассоциации [association ID (AID)]. Другими словами, станция будет идентифицировать себя для ТД и запрашивать буферизированный односторонний [unicast] кадр. Поле Duration/ID теперь используется строго в качестве идентификатора, и не используется для длительности или переустановки таймеров NAV. Только кадры опроса по сбережению электропитания [power-save poll (PS-Poll)] используют это поле в качестве AID. Процесс устаревшего управления электропитанием, использующий кадры PS-Poll, обсуждается более детально позже в этой главе.

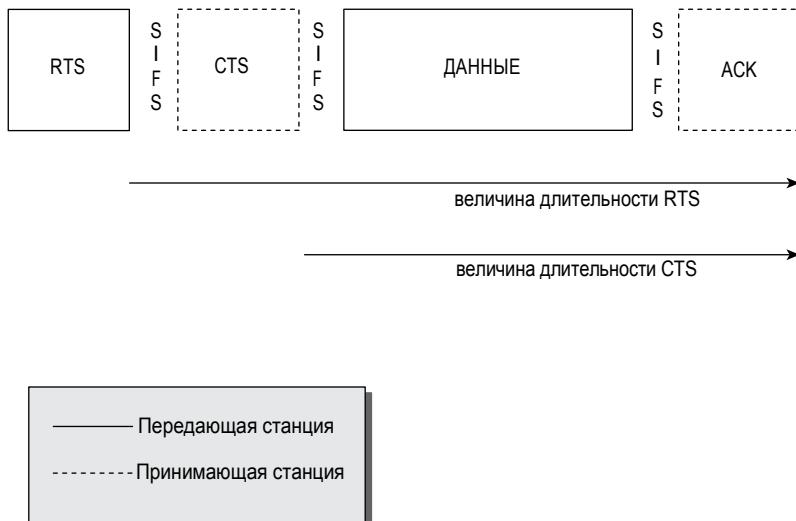
## RTS/CTS

Для того, чтобы клиентская станция приняла участие в BSS, она должна быть способна общаться с ТД. Это очевидно и логично; однако, возможно так, что клиентская станция способна общаться с ТД, но не способна слышать или быть услышанной любой другой клиентской станцией. Это может быть проблемой, потому что, как вы можете вспомнить, станция выполняет избегание конфликтов(коллизий) путем установки таймера NAV, когда она слышит другие передающие станции (виртуальный контроль несущей -virtual carrier sense) и путем прослушивания радиоэфира (физический контроль несущей -physical carrier sense). Если станция не может слышать другие станции, или она не может быть услышанной другими станциями, существует большая вероятность того, что произойдет конфликт (коллизия). *Запрос на отправку/Разрешение на отправку* (дословно: *запрос на отправку/чисто для отправки*) [Request-to-send/clear-to-send (RTS/CTS)] - это механизм, который выполняет доставку NAV и помогает предотвратить возникновение конфликтов (коллизий). Это распространение NAV резервирует среду до передачи кадра данных.

Давайте посмотрим на RTS/CTS со слегка технической точки зрения. Это будет базовое объяснение, так как глубокое объяснение находится за рамками экзамена. При использовании станцией RTS/CTS, каждый раз, когда станция хочет передать кадр, она должна выполнить обмен RTS/CTS до нормальной передачи данных. Когда передающая станция собирается передать кадр данных, она сначала отправляет кадр RTS. Значение длительности кадра RTS переустанавливает таймеры NAV всех слушающих станций так, что они должны ждать пока передаются кадры CTS, Данных и Подтверждения (ACK). Принимающая станция, ТД, затем отправляет CTS, который также используется для распространения NAV. Значение длительности кадра CTS переустанавливает таймеры NAV всех слушающих станций так, что они должны ждать пока передаются кадры Данных и Подтверждения (ACK).

Как вы можете видеть на Рисунке 9.26, значение длительности кадра RTS представляет время, в микросекундах, которое требуется для передачи обмена CTS/Данных/ACK, плюс три интервала SIFS. Значение длительности кадра CTS представляет время, в микросекундах для передачи обмена Данных/ACK, плюс два интервала SIFS. Если, какая-либо станция не слышит RTS, она должна бы слышать CTS. Когда станция слышит или RTS или CTS, она установит свой NAV таймер в предоставленное значение. В этой точке, у всех станций в BSS должны быть установлены NAV таймеры, и станции должны ждать пока не завершится полный обмен данными. Рисунок 9.27 изображает обмен RTS/CTS между клиентской станцией и ТД.

Р И С У Н О К 9 . 2 6 Величины длительности RTS/CTS

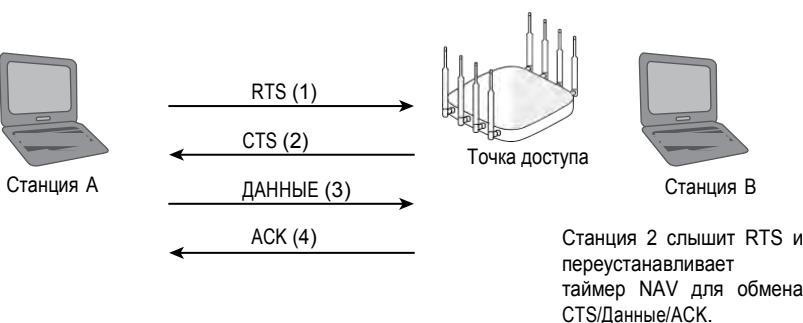


Р И С У Н О К 9 . 2 7 Обмен кадров RTS/CTS

Длительность RTS = CTS/Данные/ACK  
 длительность обмена CTS = Данные/ACK  
 длительность обмена Данных = ACK  
 Длительность ACK = 0 (обмен закончен)



Станция 3 не слышит RTS, но слышит CTS, и переустанавливает таймер NAV для обмена Данных/ACK.



RTS/CTS используются главным образом в двух ситуациях. Они могут использоваться, когда присутствует скрытый узел [hidden node] (это рассмотрено в Главе 15 “Поиск и устранение проблем в БЛВС”), или они могут быть использованы автоматически в качестве механизма защиты, когда разные технологии, такие как 802.11b/g/n, сосуществуют в одном и том же базовом составе сервиса.

## CTS-to-Self

*CTS-Самому-Себе [CTS-to-Self]* также используется автоматически в качестве механизма защиты, когда разные технологии, такие как 802.11b/g/n, сосуществуют в одном и том же базовом составе сервиса. Одно из преимуществ использования CTS-to-Self по сравнению с RTS/CTS в качестве механизма защиты – это то, что пропускная способность будет выше, из-за меньшего количества посылаемых кадров.

Когда станция, использующая CTS-to-Self, хочет передать данные, она выполняет распространение NAV путем отправки кадра CTS. Этот CTS уведомляет все другие станции, что они должны ждать, пока не завершиться обмен кадров Данные/ACK. Любая станция, которая слышит CTS установит свой NAV таймер в предоставленное значение.



CTS-to-Self лучше подходит для использования ТД, а не клиентскими станциями. Важно удостовериться, что все станции слышат CTS, чтобы зарезервировать среду, что скорее всего произойдет, если он будет отправлен ТД. Если клиентская станция использовала CTS-to-Self, есть шанс, что другая клиентская станция на противоположном конце BSS может быть очень далеко от CTS-to-Self, и не поймет, что среда занята. Даже если это правда, из нашего опыта следует, что большинство клиентских станций используют CTS-to-Self, чтобы зарезервировать среду, вместо RTS/CTS. CTS-to-Self используется из-за меньших накладных расходов [overhead], по сравнению с RTS/CTS. Некоторые производители позволяют пользователям выбрать использовать ли клиентской станции RTS/CTS или CTS-to-Self в защищенном режиме.

## Механизмы Защиты

Когда дебютировала технология 802.11g в 2006 году, стандарт 802.11 должен был обеспечить способ сосуществования технологий DSSS и OFDM в одной и той же радиосреде 2,4ГГц. Технический термин для технологии 802.11g - *Расширенная Физическая Скорость [Extended Rate Physical (ERP)]*. Радиомодуль ERP (802.11g) может эффективно работать, используя как OFDM, так и HR-DSSS передачи. Однако, старые радиомодули 802.11 или 802.11b работают только с использованием DSSS или HR-DSSS передач. Механизм защиты ERP определен так, чтобы передачи DSSS и HR-DSSS не происходили, когда два радиомодуля 802.11g работают с использованием OFDM.

Хорошей аналогией будут разговорные языки. Представьте, что радиомодуль 802.11g говорит как на Английском, так и на Испанском, в то время как радиомодуль 802.11b может говорить только по Английски. Механизм защиты ERP определен так, что когда радиомодули 802.11g говорят по Испански, радиомодули 802.11b не перебивают беседу, потому что радиомодуль 802.11b говорит только по Английски. Механизм защиты использует RTS/CTS или CTS-to-Self.

Из Главы 8, вы узнали, что один из способов предотвращения конфликтов – это установить для станций таймер с обратным отсчетом, называемым вектором сетевого распределения [network allocation vector (NAV)]. Это оповещение называется распространением NAV [*NAV distribution*]. Распространение NAV делается через поле Duration/ID, которое является частью кадра данных. Когда станция передает кадр данных, слушающие станции используют поле Duration/ID, чтобы установить свои таймеры NAV. К сожалению, по своей природе это невозможно в смешанной среде. Если устройство 802.11g передавало бы кадр данных, то устройство 802.11b было бы не способно понять данные кадра или значение Duration/ID, потому что устройства 802.11b HR-DSSS не способны понимать передачи 802.11g ERP-OFDM. Устройства 802.11b не установили бы свои таймеры NAV, и могли бы некорректно полагать, что среда доступна. Чтобы предотвратить это, станции 802.11g ERP переключаются в, что называется, *зашщщенный режим* [*protected mode*].

Как показано на Рисунке 9.28 и Рисунке 9.29, когда устройства 802.11g хотят передать данные, они сначала производят распространение NAV путем передачи обмена RTS/CTS с ТД или путем передачи CTS-to-Self, используя скорость передачи данных и метод модуляции, которые станции 802.11b HR-DSSS могут понять. В надежде, что RTS/CTS или CTS-to-Self будут услышаны и поняты всеми станциями 802.11b и 802.11g. RTS/CTS или CTS-to-Self будут содержать значение Duration/ID, которое все слушающие станции будут использовать, чтобы установить свои таймеры NAV. Если проще, то используя язык, который все станции могут понимать, устройства ERP(802.11g) уведомляют все станции о необходимости переустановить свои значения NAV. После того, как RTS/CTS или CTS-to-Self были использованы для резервирования среды, станция 802.11g может передавать кадр данных с использованием модуляции OFDM без беспокойства о конфликтах с 802.11b HR-DSSS или старыми станциями 802.11 DSSS.

**РИСУНОК 9.28** Механизм защиты—RTS/CTS

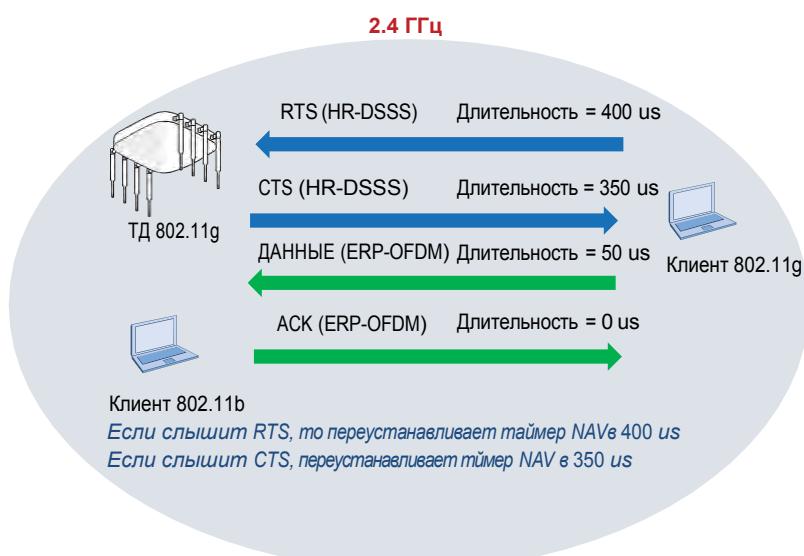
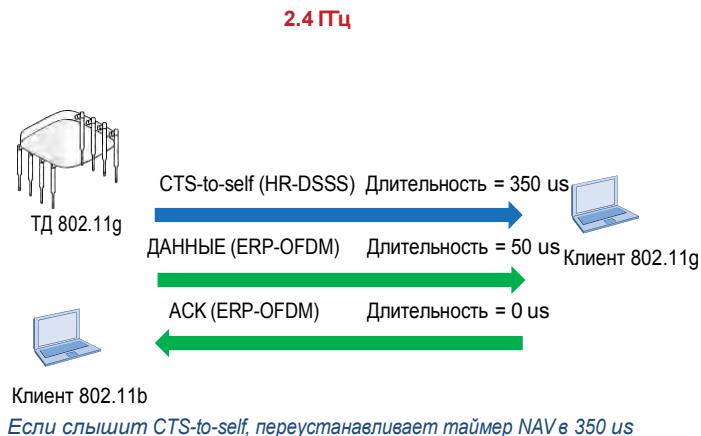


РИСУНОК 9.29 Механизм защиты—CTS-to-Self



Внутри базового состава сервиса ERP, станции HR-DSSS (802.11b) и устаревшие 802.11 DSSS называются *не-ERP станциями* (*non-ERP stations*). Назначение механизма защиты в том, чтобы станции ERP (802.11g) могли сосуществовать с не-ERP станциями (802.11b и старыми 802.11) внутри одного и того же BSS. Это позволяет ERP станциям использовать более высокие ERP-OFDM скорости передачи данных, чтобы передавать и получать данные, при этом поддерживая обратную совместимость со старыми устаревшими не-ERP станциями.

Так что же точно запускает механизм защиты ERP? Когда ТД ERP (802.11g) решает включить использование механизма защиты, ей необходимо уведомить все станции ERP (802.11g) в BSS, которым требуется защита. Она выполняет это путем установки бита NonERP\_Present (неERP\_Присутствие) в кадрах-маяках и кадрах зондирующих ответов, которые уведомляют станции ERP, которым требуется режим защиты. Существует целый набор причин почему может быть включен защищенный режим. Ниже даны три сценария, которые могут запустить защиту в базовом сервисном составе ERP:

- Если non-ERP STA ассоциирована с ТД ERP, то ТД ERP включает бит NonERP\_Present в свои собственные маяки, включая тем самым механизм защиты в своей BSS. Другими словами, ассоциация клиентов HR-DSSS (802.11b) запустит защиту.
- Если ТД ERP слышит маяк от ТД, где поддерживающие скорости передачи данных содержат только скорости 802.11b или 802.11 DSSS, то она включит бит NonERP\_Present в свои собственные маяки, включая механизм защиты в своем BSS. Простыми словами, если ТД 802.11g слышит кадр маяка от ТД 802.11 или 802.11b или клиента ad hoc, то будет запущен механизм защиты.

- Если ТД ERP слышит кадр управления (отличный от зондирующего запроса), где поддерживаемая скорость включает только скорости 802.11 или 802.11b, то бит NonERP\_Present может быть установлен в 1.

Подводя итог: Механизм защиты ERP используется так, чтобы устаревшие станции 802.11b и 802.11g могли сосуществовать в одном BSS, с использованием механизма защиты RTS/CTS и CTS-to-Self. В Главе 13, вы узнаете, что устранение устаревших клиентов 802.11b из любой БЛВС уровня предприятия является настойчиво рекомендованной практикой. Выключение скоростей передачи данных 802.11b на ТД уменьшит потребление эфирного времени [airtime] и увеличит производительность БЛВС. Если клиенты 802.11b не принадлежат BSS, то и нет необходимости в механизмах защиты RTS/CTS.

Если устранение клиентов 802.11b является лучшей рекомендованной практикой, почему тогда эта глава так подробно охватывает механизм защиты ERP? Дело в том, что механизм защиты ERP является также основой для сосуществования между устройствами 802.11n/ac/ax и раннее устаревшими устройствами. RTS/CTS и CTS-to-Self снова нужны, когда станции 802.11n/ac/ax работают в том же BSS, что и станции 802.11a/b/g. Механизм защиты HT, который также используют RTS/CTS и CTS-to-Self будет обсуждаться в Главе 10.

## Кадры Данных

Большинство кадров данных 802.11 [*802.11 data frames*] несут реальные данные, которые идет вниз от протоколов верхних уровней. Полезная нагрузка MSDU уровней 3-7 обычно зашифрована по причинам секретности. Однако, некоторые кадры данных 802.11 не несут полезную нагрузку MSDU совсем, но имеют специальное назначение MAC контроля в BSS. Любые кадры данных, которые не несут полезную нагрузку MSDU не зашифрованы, потому что данных полезной нагрузки уровней 3-7 нет.

Всего существует девять подтипов кадров данных. Два наиболее типовых кадра данных имеют подтип - *данные* [*data*] (обычно называемых как *простой кадр данных* [*simple data frame*]), и подтип - *данные с поддержкой качества сервиса* (*QoS data*). Разница между ними в том, что кадры данных с поддержкой QoS несут информацию о классе сервиса в поле QoS Control. Простые кадры данных иногда называют *не-QoS кадры данных* [*non-QoS data frames*].

Оба кадра данных инкапсулируют информацию MSDU верхних уровней в тело кадра. По причинам секретности, полезная нагрузка MSDU данных обычно зашифрована. После того, как полезная нагрузка дешифруется, интеграционный сервис, который находится в точках доступа и БЛВС контроллерах, берет полезную нагрузку MSDU кадра данных и переносит MSDU в кадры 802.3 Ethernet.

Максимальный размер тела кадра простого кадра данных или кадра данных с QoS определяется максимальным размером MSDU (2304 байта), плюс накладные расходы (overhead) от шифрования. Шифрование WEP добавляет 8 байт накладных расходов к телу кадра данных 802.11. Шифрование TKIP добавляет 20 байт накладных расходов к телу кадра данных 802.11. Шифрование CCMP добавляет 16 байт накладных расходов к телу кадра данных 802.11.

В действительности, большинство из девяти подтипов кадров данных не существуют. В Главе 8 вы узнали об optionalной функции доступа с поддержкой QoS, называемой Доступ к Каналу, Управляемый HCF [HCF Controlled Channel Access (HCCA)]. HCCA определяет механизм качества-сервиса (QoS), где ТД управляет средой путем опроса. Как об этом писали, мы не знаем ни одного производителя БЛВС, который поддерживает HCCA.

Следовательно, пять из кадров данных 802.11, определенных стандартом 802.11-2020, существуют только на бумаге. В следующем списке девяти подтипов кадров данных, мы указали все кадры данных HCCS, которые реально никогда не использовались. Первые четыре из перечисленных подтипов кадров данных являются единственными которые представляют интерес. Девять подтипов кадров данных:

- |  |   |
|--|---|
| ▪ Data (simple data frame)                   | Данные (простой кадр данных)                    |
| ▪ Null (no data)                             | Пустой (без данных)                             |
| ▪ QoS Data                                   | Данные с поддержкой QoS                         |
| ▪ QoS Null (no data)                         | Пустой кадр QoS (нет данных)                    |
| ▪ QoS Data + CF-ACK [HCCA only]              | Данные с QoS + CF-ACK [только HCCA]             |
| ▪ QoS Data + CF-Poll [HCCA only]             | Данные с QoS + CF-Poll [только HCCA]            |
| ▪ QoS Data + CF-ACK + CF-Poll [HCCA only]    | Данные с QoS + CF-ACK + CF-Poll [только HCCA]   |
| ▪ QoS CF-Poll (no data) [HCCA only]          | QoS CF-Poll (без данных) [только HCCA]          |
| ▪ QoS CF-ACK + CF-Poll (no data) [HCCA only] | QoS CF-ACK + CF-Poll (без данных) [только HCCA] |

## Кадры данных с поддержкой QoS и без-QoS

Механизмы качества сервиса (QoS) являются требованием сертификации Wi-Fi

Мультимедиа (WMM); это строго соблюдается Wi-Fi Альянсом. Любая точка доступа 802.11 уровня предприятия и большинство клиентов БЛВС, произведенных за последние 10 лет, поддерживают механизмы QoS WMM по умолчанию. Следовательно, каждый базовый состав сервиса в большинстве установок на предприятиях считается базовым составом сервиса с поддержкой качества сервиса [*quality of service basic service set (QBSS)*], а большинство современных радиомодулей считаются станциями с поддержкой QoS.

Станции с поддержкой QoS способны передавать и кадры данных с QoS, и кадры данных без QoS. Как показано в Таблице 9.3, не является чем то не обычным иметь беспроводную сеть, которая состоит из станций с поддержкой QoS и без поддержки QoS. В таком типе смешанной среды, вероятно, что устройства с поддержкой QoS будут передавать и кадры данных с QoS, и кадры данных без QoS, в зависимости от возможностей принимающей станции.

Когда устройство без поддержки QoS участвует в передаче информации в качестве передающей станции или в качестве принимающей станции, должны использоваться кадры данных без поддержки QoS [non-QoS data frame]. Широковещательные [Broadcast] кадры передаются по умолчанию как кадры без поддержки QoS [non-QoS frames], до тех пор, пока передающая станция не знает, что все станции в базовом составе сервиса (BSS) поддерживают QoS. Также как и широковещательные [broadcast] кадры, многонаправленные [multicast] кадры передаются по умолчанию как кадры без поддержки QoS [non-QoS frames], до тех пор, пока передающая станция не знает, что все станции в базовом составе сервиса, которые являются членами многонаправленной группы [multicast group] с поддержкой QoS, в обратном случае многонаправленный [multicast] кадр будет кадром с поддержкой QoS [QoS frame].

**ТАБЛИЦА 9.3** Передачи с поддержкой QoS и без поддержки QoS

Передающая Станция	Принимающая Станция	Используемый Подтип Кадра Данных
Станция без QoS (Non-QoS station)	Станция без QoS (Non-QoS station)	Простой кадр данных (без QoS (non-QoS))
Станция без QoS (Non-QoS station)	Станция с QoS (QoS station)	Простой кадр данных (без QoS (non-QoS))
Станция с QoS (QoS station)	Станция с QoS (QoS station)	Кадр данных с поддержкой QoS (QoS data frame)
Станция с QoS (QoS station)	Станция без QoS (Non-QoS station)	Простой кадр данных
Станция без QoS (Non-QoS station)	Широковещание (Broadcast)	Простой кадр данных
Станция без QoS (Non-QoS station)	Мультиicast (Multicast)	Простой кадр данных
Станция с QoS (QoS station)	Широковещание (Broadcast)	Простой кадр данных, до тех пор, пока передающая станция не знает, что все станции в BSS поддерживают QoS, а в этом случае будет использоваться кадр данных с поддержкой QoS
Станция с QoS (QoS station)	Мультиicast Multicast	Простой кадр данных, до тех пор, пока передающая станция не знает, что все станции в BSS, что являются членами мультиicast группы, поддерживают QoS, и тогда будет использоваться кадр данных с поддержкой QoS.

## Не Переносящие Данные Кадры

Как это ни странно может звучать, некоторые кадры данных 802.11 в действительности не несут никаких данных. Пустые или Нуль кадры [Null frames] и Пустые(Нуль) Кадры с поддержкой QoS [QoS Null frames] являются кадрами, не переносящими данные. Эти оба типа кадров 802.11 имеют заголовок и окончание, но не имеют тела кадра, которое переносит полезную нагрузку MSDU. Эти кадры иногда называются как *кадры нуль функции* [*null function frames*], потому что полезная нагрузка пустая (или нуль (null)), но кадры по прежнему выполняют назначение. Клиентские станции используют кадры нуль(или пустой) функции, чтобы информировать ТД об изменениях в статусе сбережения энергии путем изменения бита Управлением Электропитанием [Power Management bit]. Когда клиентская станция решает выйти за канал [go off-channel] для активного сканирования, клиентская станция отправляет кадр нуль функции к ТД с битом Управления Электропитанием [Power Management bit] установленным в 1.. Как продемонстрировано в Упражнении 9.8, когда бит Управления Питанием установлен в 1, ТД буферизирует все 802.11 кадры этого клиента. Когда клиентская станция возвращается на канал ТД, то станция отправляет следующий кадр нуль функции с битом Управлением Электропитания, установленным в 0. Далее ТД передает забуферизованные клиентские кадры. Некоторые производители также используют кадры нуль функции для реализации методов управления питанием собственной разработки.

**УПРАЖНЕНИЕ 9.8****Использование Кадров Данных**

1. Чтобы выполнить это упражнение, вам нужно сначала загрузить файл CWNA-CH9.PCAPNG с онлайн ресурса книги, который может быть доступен по адресу [www.wiley.com/go/cwnasgbe](http://www.wiley.com/go/cwnasgbe).
2. После того, как файл загружен, вам нужна программа по анализу пакетов, чтобы открыть файл. Если у вас еще не установлен анализатор пакетов на вашем компьютере, вы можете загрузить Wireshark с [www.wireshark.org](http://www.wireshark.org).
3. Using Используя анализатор пакетов, откройте файл CWNA-CH9.PCAPNG. Большинство анализаторов пакетов показывают список собранных пакетов в верхнем разделе экрана с последовательно пронумерованными кадрами в первом столбце. Разверните комментарии к пакету (packet comments) для дальнейших указаний по просмотру кадров в пакетах #97903, #34019, и #9507.
4. Прокрутите вниз список кадров и кликните кадр #97903, который является незашифрованным простым кадром данных. Посмотрите на тело кадра и посмотрите на информацию верхних уровней, такую как IP адреса и TCP порт. Эта информация видна, потому что не используется шифрование.
5. Щелкните кадр #34019, который является кадром данных с поддержкой качества сервиса (QoS). Посмотрите на заголовок 802.11 MAC и посмотрите на поле Контроля Качества Сервиса (QoS Control). Заметьте, что уровень приоритета установлен в обычный трафик [Best Effort].
6. Кликните кадр #9507, который является кадром нуль функции. Посмотрите на заголовок 802.11 MAC. Посмотрите на поле Контроля Кадра [Frame Control] и обратите внимание, что бит Управления Питанием [Power Management] установлен в 1. Теперь ТД буферизирует клиентский трафик.

## Управление электропитанием

Одно из основных использований беспроводной сети - это обеспечение мобильности для клиентской станции. Клиентская мобильность идет рука об руку с клиентскими станциями работающими от аккумуляторных батарей. Когда используются устройства, работающие от батарей, одна из самых больших забот - это как долго продержаться батареи до того, когда нужно будет их перезарядить. Чтобы увеличить время жизни батареи, может быть использована большая, с большей длительностью, батарея, или можно уменьшить потребление энергии. Стандарт 802.11 включает возможности управления питанием, которые могут быть включены, чтобы помочь увеличить жизнь батареи. Жизнь батареи чрезвычайно важна для смартфонов, планшетов, ручных сканеров, и VoWiFi телефонов. Жизнь батареи мобильных устройств обычно должна длиться хотя бы одну 8и часовую смену. Два устаревших режима управления питанием, которые поддерживались стандартом 802.11, это активный режим и режим сбережения энергии. Методы управления питанием 802.11 также были улучшены принятой поправкой 802.11e-2005, и принятой поправкой 802.11n-2009. Дальнейшие улучшения управления питанием определены поправкой 802.11ac-2013 и поправкой 802.11ax.

## Устаревшее Управление Питанием

*Активный режим [Active mode]* это устаревший режим управления питанием, использовавшимся очень старыми станциями 802.11. Когда станция работает в активном режиме, беспроводная станция всегда готова передать или принять данные. Активный режим не обеспечивает экономии батареи. В MAC заголовке кадра 802.11, поле Управление Питанием имеет 1 бит в длину и используется для обозначения режима управления питанием станции. Значение 0 показывает, что станция находится в активном режиме. Станции, работающие в активном режиме, будут получать большую пропускную способность по сравнению со станциями, работающими в режиме экономии энергии, но жизнь батареи обычно будет намного короче.



Станции, которые всегда подключены к источнику питания, следует настраивать на использование активного режима.

*Режим экономии энергии [Power-save mode]* является опциональным режимом для станций 802.11. Когда клиентская станция работает в режиме экономии энергии, она выключает некоторые компоненты приемопередатчика на некоторый период времени, чтобы сэкономить энергию. Беспроводной радиомодуль в основном не надолго засыпает. Станция показывает, что она использует режим экономии энергии путем изменения значения бита Управление Питанием [Power Management] на 1. Когда бит Управления Питанием установлен в 1, ТД уведомлена, что клиентская станция использует управление питанием, и ТД буферизирует все кадры 802.11 этого клиента.

## Карта Индикации Наличия Трафика

Если станция является частью базового состава сервиса, она уведомит ТД, что она включила режим экономии энергии путем изменения поля Управления Питанием [Power Management] в 1. Когда ТД получает кадр от станции с этим битом, установленным в 1, ТД знает, что станция находится в режиме экономии энергии. Если ТД затем получает какие-либо данные, которые предназначены для станции в режиме экономии энергии, то ТД сохраняет информацию в буфере. Каждый раз, когда станция ассоциируется с ТД, станция получает *идентификатор ассоциации [association identifier (AID)]*. ТД использует этот AID для хранения статуса станций, которые ассоциированы и являются членами BSS. Если ТД буферизирует данные для станции в режиме экономии энергии, то когда ТД передает свой следующий маяк, AID станции будет указан в поле кадра маяка, которое называется *карта индикации наличия трафика [traffic indication map (TIM)]*. Поле TIM - это список всех станций, у которых есть еще не доставленные данные, забуферизованные ТД, и ожидающие доставку. Каждый маяк будет включать AID станций, до тех пор, пока данные не будут доставлены.

После того как станция уведомит ТД, что она находится в режиме экономии энергии, станция выключается часть своего приемопередатчика для сохранения энергии. Станция может быть в одном из двух состояний, проснувшемся [awake] или сонном [doze]

- Во время проснувшегося [awake] состояния, клиентская станция может получать и передавать кадры.
- Во время сонного [doze] состояния, клиентская станция не может получать или передавать какие-либо кадры, и работает в состоянии очень низкой энергии, чтобы сберечь энергию.

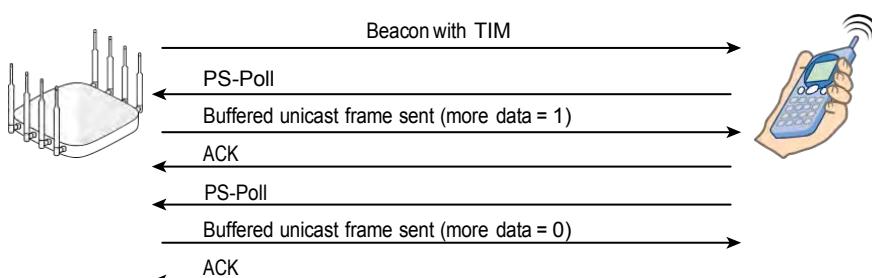
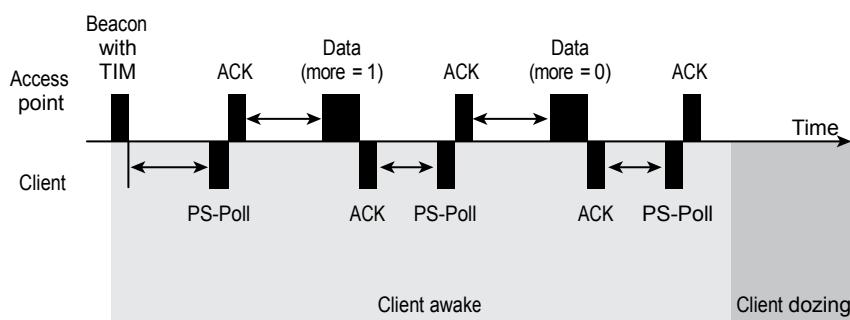
Так как маяки передаются с постоянным предопределенным интервалом, называемым

целевым временем передачи маяка [target beacon transmission time (TBTT)], все станции знают, когда будут появляться маяки. Станция остается спящей на короткий период времени и просыпается во время, чтобы услышать кадр маяк.

Станция не должна просыпаться для каждого маяка. Чтобы сберечь больше энергии, станция может спать дольший период времени, и затем проснуться в определенное время, чтобы услышать предстоящий маяк. Как часто просыпаться клиентской станции основывается на клиентской переменной, называемой *интервал прослушивания* [*listen interval*], и обычно зависит от производителя.

Как показано на Рисунке 9.30, когда станция принимает маяк, она проверяет есть ли ее AID в карте индикации наличия трафика [TIM], показывающей, что буферизированные однонаправленные [unicast] кадры ждут. Если так, то станция остается бодрой [awake] и посылает контрольный кадр PS-Poll к ТД. Внутри кадра PS-Poll поле Duration/ID используется в качестве значения идентификатора ассоциации [AID]. Другими словами, станция идентифицирует себя для ТД и запрашивает забуферизованные однонаправленные [unicast] кадры. Когда ТД получает кадр PS-Poll, она отправляет буферизированные однонаправленные данные станции. Станция остается бодрой [awake] до тех пор, пока ТД передает буферизированные однонаправленные [unicast] кадр. Когда ТД отправляет данные станции, станции нужно знать, когда все буферизированные однонаправленные [unicast] данные получены, чтобы она могла снова пойти спать. Каждый однонаправленный [unicast] кадр содержит 1-битовое поле, называемое "Есть Еще Данные" [More Data]. Когда станция получает буферизированный однородный [unicast] кадр с полем "Есть Еще Данные" [More Data], установленным в 1, станция знает, что она не может еще пойти спать, потому что есть еще буферизированные данные, которые еще не получены. Когда поле "Есть Еще Данные" [More Data] установлено в 1, станция знает, что ей нужно послать следующий кадр PS-Poll, и ждать, чтобы получить следующий буферизированный однородный кадр.

**РИСУНОК 9.30** Устаревшее управление питанием



После того, как все буферизированные однонаправленные кадры переданы, поле "Есть Еще Данные" [More Data] в последнем буферизированном кадре будет установлено в 0, обозначающее, что больше буферизированных данных нет, и станция пойдет спать. ТД установит значение бита AID станции в 0, и когда придет следующий TBTT, ТД отправит маяк. Станция останется в состоянии сна на небольшой период времени, а затем снова проснеться в определенное время, чтобы услышать кадр маяк. Когда станция получает маяк, она снова проверяет есть ли ее AID в TIM. Допустим, что нет буферизированных однонаправленных кадров, ожидающих эту станцию, тогда AID станции не будет установлен в 1 в TIM, и станция сможет просто вернуться ко сну, пока не наступит время проснуться и снова проверить.

## Карта Индикации Доставки Трафика

В дополнение к одноточечному [unicast] трафику, сетевой трафик включает многонаправленный [multicast] и широковещательный [broadcast] трафик. Так как многовещательный и широковещательный трафик направлен ко всем станциям, то BSS необходимо обеспечить способ, чтобы гарантировать, что все станции проснулись, чтобы получить эти кадры. *Карта индикации доставки трафика [delivery traffic indication map (DTIM)]* используется, чтобы гарантировать, что все станции, использующие управление питанием, проснулись, когда отправляется многовещательный или широковещательный трафик. DTIM – это специальный тип TIM. TIM или DTIM передается как часть каждого маяка.

Конфигурируемые настройки на ТД, называемые *интервал DTIM [DTIM interval]* определяют как часто передается маяк DTIM. Интервал DTIM 3 означает, что каждый третий маяк является маяком DTIM, а DTIM интервал 1, означает, что каждый маяк является маяком DTIM. Каждый маяк содержит информацию DTIM, которая информирует станции, когда будет следующий DTIM. Значение DTIM 0 обозначает, что текущий TIM – это DTIM. Все станции проснутесь во время, чтобы получить маяк с DTIM. Если у ТД есть многонаправленный [multicast] или широковещательный [broadcast] трафик для отправки, она передает маяк с DTIM и затем немедленно посыпает многонаправленные или широковещательные данные.

После того как многонаправленные [multicast] или широковещательные [broadcast] данные переданы, если AID станции был в DTIM, то станция остается бодрой [awake] и пошлет кадр PS-Poll и продолжит получать свой буферизированный одноточечный [unicast] трафик от ТД. Если станция не увидела свой AID в DTIM, или если ее AID был установлен в 0, то станция может идти обратно спать.

Интервал DTIM является важным для любого приложения, которое использует многонаправленное вещание [multicasting]. Например, много производителей VoWiFi поддерживают функцию *нажми-чтобы-говорить [push-to-talk]*, которая посылает трафик VoIP на мультикастный адрес. Неправильно настроенный интервал DTIM может вызвать проблемы с производительностью во время многонаправленного вещания нажми-чтобы-говорить (push-to-talk multicast).

## Энергосбережение WMM и U-APSD

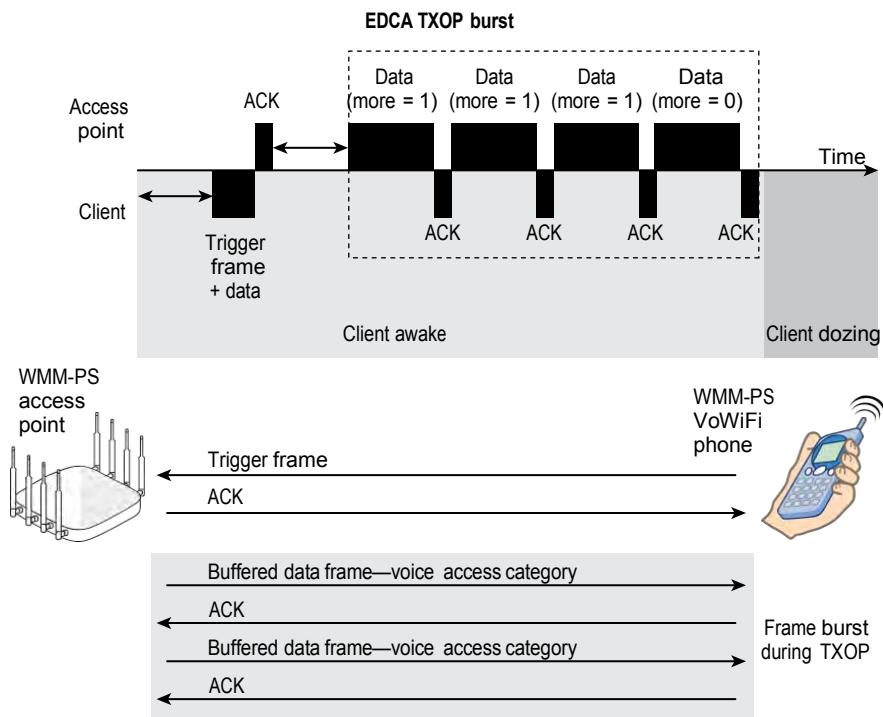
Главный фокус поправки 802.11e, которая теперь является частью стандарта 802.11-2020, это качество сервиса. Однако, поправка IEEE 802.11e также представила расширенный метод управления питанием, который называется *автоматическое энергосбережение [automatic power save delivery (APSD)]*. Два метода ASPD, которые определены – это: *автоматическое энергосбережение по-расписанию [scheduled automatic power save delivery (S-APSD)]* и *незапланированное автоматическое энергосбережение [unscheduled automatic power save delivery (U-APSD)]*. Метод управления питанием S-APSD находится за пределами этой книги. Сертификация Wi-Fi Альянса WMM-Энергосбережение [*WMM-Power Save (WMM-PS)*] основана на U-APSD. WMM-PS является улучшение устаревших механизмов сбережения энергии, которые уже обсуждались. Цель WMM-PS заставить клиентские устройства проводить больше времени в состоянии сна и потреблять меньше энергии. WMM-PS также разработан, чтобы минимизировать задержку для чувствительных ко времени приложений, таких как голос, во время процесса управления питанием.

Устаревшие методы управления питанием имеют несколько ограничений. Как показано на Рисунке 9.30, клиент, использующий устаревшее управление питанием, должен сначала ждать маяк с TIM, прежде чем клиент сможет запросить буферизированные односторонние [unicast] кадры. Клиент также должен отправить уникальный кадр PS-Poll к ТД, чтобы запросить каждый отдельный буферизированный односторонний [unicast] кадр. Этот пинг-понг метода управления питанием увеличивает задержку чувствительных ко времени приложений, таких как голос. Клиенты также должны оставаться не спящими [awake] во время пинг-понг процесса, что приводит к уменьшению жизни батареи. Кроме того, количество времени, которое клиенты проводят в спящем режиме, определяется драйвером производителя, а не трафиком приложения.

WMM-PS использует спусковой или триггерный [trigger] механизм, чтобы получить буферизированный односторонний [unicast] трафик, базирующийся на категориях доступа WMM. Вы знаете из Главы 8, что используются метки приоритета [priority tags] 802.1D со стороны Ethernet, чтобы направить трафик по четырем различным приоритетным очередям по категориям доступа WMM.

Очереди по категориям доступа это – для голоса [voice], для видео [video], для негарантированного трафика [best effort], для фоновых данных [background]. Как показано на Рисунке 9.31, клиентская станция посыпает триггерный кадр, относящийся к категории доступа WMM, чтобы проинформировать ТД, что клиент проснулся и готов загрузить любые кадры, которые ТД могла забуферизовать для этой категории доступа. Триггерный кадр может также быть кадром данных 802.11, таким образом устраняя необходимость в отдельном кадре PS-Poll. ТД затем отправит ACK клиенту, и продолжит посыпать «взрыв кадров» буферизированного трафика приложения во время возможности передачи (TXOP).

РИСУНОК 9.31 WMM-PS



Преимущества этого улучшенного метода управления питанием включает следующее:

- Теперь приложения управляют поведением энергосбережения путем установки периодов сна и отправки триггерных кадров. Телефоны VoWiFi очевидно отправляют триггеры ТД часто во время голосового вызова, в то время как радиомодуль ноутбука, использующий приложения данных, будет иметь более долгие периоды сна.
- Методы запуска [trigger] и доставки [delivery] устраниют необходимость в кадрах PS-Poll.
- Клиент может запросить загрузку буферизированного трафика и не ждать кадр маяк.
- Весь исходящий [downlink] трафик приложения отправляется в более быстрые взрыве кадров во время TXOP ТД.

Должны выполняться пара условий, чтобы Wi-Fi клиент использовал улучшенные механизмы WMM-PS:

- Клиент должен быть СЕРТИФИЦИРОВАННЫМ Wi-Fi для WMM-PS [Wi-Fi CERTIFIED for WMM-PS].
- ТД должна быть СЕРТИФИЦИРОВАННОЙ Wi-Fi для WMM-PS.

Стоит отметить, что приложения, которые не поддерживают WMM-PS, могут сосуществовать с приложениями с включенным Энергосбережением WMM [WMM-Power Save]. Данные от других приложений будут доставляться устаревшими методами управления питанием.

## Управление Питанием в MIMO

Принятая поправка 802.11n-2020 определяет два метода управления питанием, которые могут быть использованы радиомодулями с несколькими входами, несколькими выходами [multiple-input, multiple-output (MIMO)]. Первый метод называется *энергосбережение с пространственным мультиплексированием* [*spatial multiplexing power save (SM power save)*]. Цель Энергосбережения с Пространственным Мультиплексированием [SM power save] заключается в том, чтобы позволить устройству MIMO 802.11n/ac выключить все свои, кроме одной, радиоцепи. Более детальное обсуждение о методах управления питанием MIMO представлено в Главе 10. В Главе 19 “802.11ax: Высокая Эффективность” вы узнаете о дополнительных улучшениях в управлении питанием, которые помогут сохранить жизнь аккумуляторной батареи для устройств IoT.

## Управление Питанием в 802.11ax

Все эти методы управления питанием определяют разные способы перехода между состояниями “бодрствования” [“awake”] и “сна” [“sleep”] для радиомодуля клиента. Когда радиомодуль клиента спит, энергия не нужна, и следовательно, рабочая жизнь батареи продлевается. Запомните, что радиомодули клиента не спят часами или даже минутами. Типовая длительность сна может измеряться микросекундами. Когда клиентский радиомодуль использует управление питанием [power management], переход между состояниями “бодрствования” и “сна” непрерывен. Однако, кумулятивный эффект от непрекращающихся состояний сна сохраняет жизнь батареи.

Одно исключение в этом процессе – это новый метод управления питанием, определенный для радиомодулей 802.11ax. *Целевое время пробуждения* [*Target wake time (TWT)*] является улучшенным механизмом управления питанием в Wi-Fi 6. TWT – это обсуждаемое соглашение, основанное на ожидаемой активности трафика между точкой доступа и клиентами, для определения запланированного целевого времени пробуждения для клиентов Wi-Fi 6 режиме энергосбережения [power-save (PS) mode]. TWT может теоретически позволить клиентским устройствам засыпать на часы. TWT является идеальным методом энергосбережения для устройств IoT, которым необходимо сохранить жизнь батареи. Более глубокое обсуждение процедур энергосбережения TWT можно найти в Главе 19.

## Итого

Эта глава охватила следующие ключевые области архитектуры MAC:

- Формат кадра 802.11 802.11 frame format
  - Основные типы кадров 802.11 Major 802.11 frame types
  - Подтипы кадров 802.11 802.11 frame subtypes
  - Машина состояний 802.11 802.11 state machine
  - Механизмы защиты Protection mechanisms
  - Управление Питанием Power management

Важно понимать состав трех основных типов кадров 802.11, и назначение каждого отдельного кадра 802.11, и как они используются при сканировании, аутентификации, ассоциации, и других MAC процессах. Вам следует понимать необходимость обоих механизмов защиты RTS/CTS и CTS-to-Self.

Чтобы помочь управлять жизнью батареи, на беспроводной станции может быть настроено управление питанием [power management]. Активный режим не предоставляет никакого вида сохранения батареи, в то время как режим энергосбережения [power-save mode] может быть неоценим для увеличения жизни батарей ноутбука и ручных вычислительных устройств. WMM и 802.11n также имеют улучшенные возможности управления питанием. Мы обсудили следующие части управления питанием в этой главе:

- Кarta индикации наличия трафика [Traffic indication map (TIM)]
  - Кара индикации доставки трафика [Delivery traffic indication map (DTIM)]
  - Энергосбережение WMM [WMM-Power Save (WMM-PS)]

## Темы Экзамена

**Объяснить различия между PPDU, PSDU, MPDU, и MSDU.** Понимать на каком уровне модели OSI работает каждый блок данных, и что каждый блок данных содержит.

**Понимать формат кадра 802.11.** Описать ключевые компоненты MAC заголовка 802.11. Быть способным объяснить MAC адресацию 802.11. Понимать, что окончание 802.11 используется для целостности данных.

**Знать три основных типа кадров 802.11.** Убедитесь, что вы знаете функции кадров управления, контроля и данных. Знать, что делает основные типы кадров разными.

Кадры данных содержат MSDU, когда кадры управления и контроля не содержат.

Понимать назначение каждого отдельного подтипа кадров рассмотренных в этой главе.

**Знать процесс контроля доступа к среде [media access control (MAC)] и все кадры, которые используются во время этого процесса.** Понимать функцию каждого из перечисленного: активное сканирование, пассивное сканирование, маяк, зондирующий запрос, зондирующий ответ, аутентификация, ассоциация, переассоциация, деассоциация и деаутентификация.

**Знать важность кадров ACK для определения, что однокаправленный [unicast] кадр был получен и неповрежден.** Понимать, что после того, как передан однокаправленный кадр, идет короткое межкадровое пространство [short interframe space (SIFS)], а затем приемная станция отвечает передачей ACK.

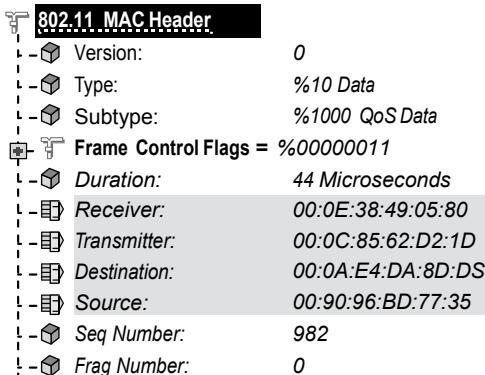
Если этот процесс завершен успешно, то передающая станция знает, что кадр был получен и не был поврежден. Понимать, что блоковые ACK используются с взрывами кадров и агрегацией кадров A-MPDU.

**Понимать важность механизмов защиты и того как они работают.** Механизмы защиты используют контрольные кадры RTS/CTS или CTS-to-Self, чтобы очистить канал. Исходное назначение механизма защиты было в том, чтобы станции ERP (802.11g) могли существовать с не-ERP станциями (802.11b и устаревшими 802.11) внутри одного и того же BSS. Однако, защита RTS/CTS и CTS-to-Self также используется, когда станции 802.11n/ac работают в том же самом BSS, что и станции 802.11a/b/g.

**Понимать все технологии, которые образуют управление питанием.** Управление питанием может быть включено для уменьшения использования энергии и увеличения срока жизни батареи. Понимать как буферизированный однокаправленный трафик принимается различными способами: от буферизированного широковещательного [broadcast] и многонаправленного [multicast] трафика. Понимать улучшения управления питанием, определенные в WMM-PS.

## Контрольные Вопросы

1. Какой из следующих кадров 802.11 несет полезную нагрузку MSDU, которая может фактически быть перенесена интеграционным сервисом в кадр Ethernet 802.3?
  - A. Кадры управления 802.11 (802.11 management frames)
  - B. Кадры контроля 802.11 (802.11 control frames)
  - C. Кадры данных 802.11 (802.11 data frames)
  - D. Кадры действия 802.11 (802.11 action frames)
  - E. Кадры ассоциации 802.11 (802.11 association frames)
2. Что из перечисленного содержит только данные LLC и IP пакет, и не включает никакие данные 802.11 уровня 2?
  - A. MPDU
  - B. PPDU
  - C. PSDU
  - D. MSDU
  - E. MMPDU
3. Основываясь на перехваченном кадре 802.11, показанном здесь, какой тип сетевой (связи) коммуникации происходит?



- A. ТД к клиентской станции
- B. Клиентской станции к серверу
- C. Клиентской станции к ТД
- D. Сервера к клиентской станции
- E. ТД к ТД

- 4.** Присутствие какого типа передачи может запустить механизм защиты в базовом составе сервиса ERP ? (Выберите все, что применимо.)
- A.** Ассоциация клиента HR-DSSS
  - B.** Ассоциация клиента ERP-OFDM
  - C.** Кадр маяк [beacon] HR-DSSS
  - D.** Кадр маяк [beacon] ERP с битом NonERP\_Present, установленным в 1
  - E.** Ассоциация клиента FHSS
- 5.** Какая из нижеследующей информации включена в кадр зондирующего ответа [probe response]? (Выберите все, что применимо.)
- A.** Информация о канале
  - B.** Поддерживаемые скорости передачи данных [Supported data rate]
  - C.** Базовые скорости передачи данных [Basic data rates]
  - D.** SSID
  - E.** Карта индикации наличия трафика [Traffic Indication Map]
- 6.** Какое из следующих выражений является верным о кадре управления маяк (beacon)? (Выберите все, что применимо.)
- A.** Маяки могут быть выключены, чтобы скрыть сеть от проникновения в неё.
  - B.** Информация отметок времени используется клиентами для синхронизации своих часов.
  - C.** В BSS клиенты делят ответственность за передачу маяков
  - D.** Маяки могут содержать proprietарную информацию производителя
- 7.** Какое из следующих выражений относительно четырех полей MAC адресов в MAC заголовке 802.11 является точным? (Выберите все, что применимо.)
- A.** Адрес 2 всегда является адресом передатчика [transmitter address (TA)].
  - B.** Адрес 3 всегда является адресом передатчика [transmitter address (TA)].
  - C.** Адрес 1 всегда является идентификатором базового состава сервиса [basic service set identifier (BSSID)].
  - D.** Адрес 1 всегда является адресом приемника [receiver address (RA)].
  - E.** Адрес 3 всегда является идентификатором базового состава сервиса (basic service set identifier [ BSSID]).
  - F.** Адрес 2 всегда является адресом приемника [receiver address (RA)].
- 8.** Когда станция посыпает RTS, поле Duration/ID уведомляет другие станции о том, что они должны установить свой таймер NAV в какое из следующих значений?
- A.** 213 микросекунды
  - B.** Время, необходимое для передачи кадров Данных и ACK
  - C.** Время, необходимое для передачи кадра CTS
  - D.** Время, необходимое для передачи кадров CTS, Данных, и ACK.

9. Как клиентская станция показывает, что она использует режим энергосбережения [power-save mode]?
- A. Она передает кадр к ТД с полем Сон [Sleep], установленным в 1.
  - B. Она передает кадр к ТД с полем Управление Питанием [Power Management] установленным в 1.
  - C. Используя DTIM, ТД определяет, когда клиентская станция использует режим энергосбережения.
  - D. Ей не нужно это, потому что режим энергосбережения существует по умолчанию.
10. Что заставит станцию 802.11 повторно передать [retransmit] однокапельный [unicast] кадр? (Выберите все, что применимо.)
- A. Переданный однокапельный [unicast] кадр был поврежден.
  - B. Кадр ACK от приемника был поврежден
  - C. Буфер приемника был полон.
  - D. Буфер передающей станции был полон.
11. Если станция в режиме энергосбережения [power-save mode], как она узнает, что у ТД есть буферизированные однокапельные [unicast] кадры, ожидающие ее?
- A. Путем проверки кадра PS-Poll
  - B. Путем проверки поля TIM
  - C. Когда она принимает ATIM
  - D. Когда бит Управления Питанием [Power Management] установлен в 1
  - E. Путем проверки интервала DTIM
12. Когда стандарт IEEE 802.11-2020 требует от ТД 802.11ac, передающей на 5ГГц, ответить на кадры зондирующего запроса от соседних клиентских станций? (Выберите все, что применимо.)
- A. Когда кадры зондирующего запроса содержат пустое [null] значение SSID.
  - B. Когда клиент зондирующего запроса также является радиомодулем 802.11ac
  - C. Когда зондирующий запрос зашифрован
  - D. Когда в зондирующем запросе бит Управления Питанием [Power Management] установлен в 1
  - E. Когда кадры зондирующего запроса содержат корректное значение SSID
13. Какие из следующих выражений о сканировании являются верными? (Выберите все, что применимо)
- A. Существует два типа сканирования: пассивное и активное.
  - B. Станции должны передавать маяки для того, чтобы узнать о локальных ТД.
  - C. Стандарт 802.11 позволяет ТД игнорировать пилотные запросы по причинам безопасности.
  - D. Является обычным делом для станций продолжать посыпать пилотные запросы, после ассоциации с ТД.
14. Дано, что MAC заголовок 802.11 может иметь до четырех MAC адресов, какие типы адресов на находятся в MAC заголовке 802.3? (Выберите все, что применимо)
- A. SA
  - B. BSSID
  - C. DA

- D.** RA  
**E.** TA
- 15.** Когда клиентская станция впервые включена, какой порядок кадров генерируется клиентской станцией и ТД?
- A.** Зондирующий запрос/ответ [Probe request/response], Запрос/ответ на ассоциация [association request/response], запрос/ответ на аутентификацию [authentication request/response]
- B.** Зондирующий запрос/ответ [Probe request/response], запрос/ответ на аутентификацию [authentication request/response], запрос/ответ на ассоциацию [association request/response]
- C.** Запрос/ответ на ассоциацию [Association request/response], запрос/ответ на аутентификацию [authentication request/response], зондирующий запрос/ответ [probe request/response]
- D.** Запрос/ответ на аутентификацию [Authentication request/response], запрос/ответ на ассоциацию [association request/response], зондирующий запрос/ответ [probe request/response]
- 16.** Пользователи БЛВС недавно жаловались на провалы в звуке [audio] и проблемы с функцией «нажми-чтобы-говорить» (push-to-talk) с VoWiFi телефонами компании ACME. Что может быть причиной этой проблемы?
- A.** Неправильные настройки TIM  
**B.** Неправильные настройки DTIM  
**C.** Неправильные настройки ATIM  
**D.** Неправильные настройки BTIM
- 17.** Служба поддержки БЛВС приняла звонок о том, что внезапно все беспроводные сканеры штрих-кодов с устаревшим 802.11b не могут подключиться ни к какой ТД 802.11n. Однако, все клиент 802.11g/n все еще могут подключаться. Что является возможной причиной этой проблемы? (Выберите все, что подходит.)
- A.** Администратор БЛВС выключил скорости передачи данных 1, 2, 5.5, и 11 Мбит/с.  
**B.** Администратор БЛВС выключил скорости передачи данных 6 и 9 Мбит/с.  
**C.** Администратор БЛВС включил скорости передачи данных 6 и 9 Мбит/с в качестве базовых скоростей (basic rates).  
**D.** Администратор БЛВС настроил все ТД на бой канал.
- 18.** Какой из этих кадров данных 802.11 несет полезную нагрузку MSDU? (Выберите все, что подходит.)
- A.** Кадр данных без QoS [Non-QoS data frame]  
**B.** Кадр данных с QoS [QoS data frame]  
**C.** Пустой кадр [Null frame]  
**D.** Пустой кадр с QoS [QoS null frame]
- 19.** Что является примером того, как кадр действия может быть использован?

**386** Глава 9 • 802.11 MAC  
(Выберите все, что применимо.)

- A.** Кадр действия может функционировать как зондирующий запрос (probe request).
  - B.** Кадр действия может функционировать как запрос отчета о соседях (neighbor report request).
  - C.** Кадр действия может функционировать как зондирующий ответ (probe response).
  - D.** Кадр действия может функционировать как оповещение о переключении канала.
  - E.** Кадр действия может функционировать как маяк (beacon).
- 20.** Какое заключение вы можете сделать об этом кадре, основываясь на перехваченном кадре, на показанном кадре? (Выберите все, что применимо)

-802.11

```
Frame Control: 0x0A08 (2568)
└ Protocol version: 0
└ To DS: 0
└ From DS: 1
└ More Fragments : 0
└ Retry: 1
└ Power Management: 0
└ More Data: 0
└ Protected Frame: 0
└ Order: 0
└ Type: 2 - Data
└ Subtype: 0 - Data
Duration: 0x002C (44)
Destination Address: 00:20:A6:4F:A9:BE
BSS ID: 00:0C:6E:5A:47:D5
Source Address: 00:04:5A:64:87:2A
Fragment Number: 0x0000 (0)
Sequence Number: 0x001D (29)
```

- A.** Это однокомандный (unicast) кадр.
- B.** Это многокомандный (multicast) кадр.
- C.** Это широковещательный (broadcast) кадр.
- D.** Это передача между взаимосвязанной (mesh) точкой ТД и взаимосвязанным (mesh) порталом (ТД).
- E.** Этот кадр зашифрован.
- F.** Последовательность Кадровой Проверки (FCS) предыдущей попытки того же самого кадра провалилась на приемной станции.

# Глава 10



## Технология **MIMO: HT и VHT**

**В ЭТОЙ ГЛАВЕ ВЫ УЗНАЕТЕ О  
СЛЕДУЮЩЕМ:**

✓ **MIMO**

- Радиотехнические цепи
- Пространственное мультиплексирование
- Сравнение разнесений MIMO и SISO
- Комбинация максимального отношения
- Пространственно-временное блочное кодирование
- Разнесение циклического сдвига
- Формирование луча по Передаче
- Подробное формирование луча

✓ **Многопользовательское MIMO**

- Многопользовательское формирование луча

✓ **Каналы**

- Каналы 20 МГц
- Каналы 40 МГц
- Сорокамегагерцевая нетолерантность
- Каналы 80 МГц и 160 МГц

✓ **Захитный Интервал**

✓ **Модуляция 256-QAM**

✓ **802.11n/ac PPDUs**

- Не-HT [Non-HT]
- Смешанный HT [HT Mixed]
- VHT



✓ **802.11n/ac MAC**

- A-MSDU
- A-MPDU
- Блоковое подтверждение
- Управление питанием
- Схема модуляции и кодирования
- Скорости передачи данных 802.11ac

✓ **Механизмы защиты HT/VHT**

- Режимы защиты HT(0–3)

✓ **Сертификация Wi-Fi Альянса**



В этой главе, мы обсуждаем основанные на MIMO Wi-Fi технологии: высокая пропускная способность [*high throughput(HT)*], изначально определенная поправкой 802.11n-2009, и очень высокая пропускная способность [*very high throughput (VHT)*], изначально определенная поправкой 802.11-2013.

Обе технологии предоставили улучшения PHY и MAC вместе с увеличенной скоростью передачи данных. Эта глава фокусируется на технологиях HT и VHT, предоставляя крепкий фундамент для понимания MIMO, которая также является центральной технологией для 802.11ax, последнего 802.11 PHY. 802.11ax в значительной степени объяснено в Главе 19 "802.11ax: Высокая Эффективность".

Исходная главная цель поправки 802.11n была в увеличении скоростей передачи данных и пропускной способности в обоих полосах частот 2,4Гц и 5ГГц. Поправка 802.11n определяет рабочий режим, который называется *высокая пропускная способность [high throughput (HT)]*, в котором характеристики PHY и MAC улучшены, чтобы потенциально обеспечить скорость передачи до 600Мбит/с. Поправка 802.11ac определила новый рабочий режим, названный *очень высокая пропускная способность [very high throughput (VHT)]*. VHT работает только в полосах U-NII 5ГГц и предоставляет улучшения PHY и MAC, которые позволяют потенциально получить скорости передачи до 6933,3Мбит/с.

802.11n ввел целиком новый подход к Физическому уровню, используя технологию, названную *много-вводов, много выводов [multiple-input, multiple-output (MIMO)]*, которая требует использование нескольких радиомодулей и антенн. Радиомодули 802.11n и 802.11ac используют технологию MIMO, которая использует преимущества многолучевых [*multipath*] сигналов, чтобы увеличить пропускную способность и диапазон.

Помимо использования технологии МИМО, механизмы HT и VHT обеспечивают расширенную пропускную способность, используя и другие методы. Мы обсудим использование более широких каналов, которые предлагают большую ширину полосы частот. Улучшения в MAC подуровне также обеспечивают большую пропускную способность с использованием агрегации кадров. Поправка 802.11e определяет улучшения в управлении питанием, а позже, поправка 802.11n также определяет новый механизм управления питанием.

802.11ac расширила и в некоторых случаях упростила многие из технологий 802.11n, вместе с тем введя новую технологию, называемую *многопользовательский MIMO [multi-user MIMO (MU-MIMO)]*. MU-MIMO позволяет обеспечить связь некоторым пользователям в исходящем канале связи [*downlink*] от точки доступа (ТД) к некоторым клиентам во время одной и той же возможности передачи [*transmission opportunity (TXOP)*]. Для большей части, 802.11ac был улучшением или расширением 802.11n, расширяющим возможности 802.11n, обеспечивающим более быстрый Wi-Fi. Таблица 10.1 приводит краткий итог по различию между 802.11n и 802.11ac.

390 Глава 10 • Технология MIMO: HT и VHT  
**ТАБЛИЦА 10.1** Сравнение 802.11n и 802.11ac

Технология	802.11n - HT	802.11ac - VHT
Частота	2.4 ГГц и 5 ГГц	только 5 ГГц
Модуляция	BPSK, QPSK, 16-QAM, 64-QAM	BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM
Ширины каналов	20 МГц, 40 МГц	20 МГц, 40 МГц, 80 МГц, 160 МГц
Пространственные потоки	До четырех	До восьми на ТД, до четырех на клиентов
Поддержка короткого защитного интервала	Да	Да
Формирование луча	Несколько типов, и явный и неявный; обычно не применяется	Явное формирование луча пакетами с пустыми(null) данными (NDPs)
Количество схем модуляций и кодирования (MCSs)	77	10
Поддержка A-MSDU и A-MPDU	Да	Да, все кадры передаются как A-MPDU
Поддержка MIMO	Одно пользовательский MIMO	Однопользовательский MIMO, и многопользовательский MIMO (MU-MIMO)
Максимальное количество одновременных пользовательских передач	Один	Четыре
Максимальная скорость передачи данных	600 Мбит/с	6933.3 Мбит/с

Наконец, мы обсуждаем различные режимы работы сетей HT и VHT, и как их радиопередачи могут сосуществовать в одной и той же среде БЛВС с радиомодулями, которые используют не-MIMO технологии. В этой главе, мы охватим ключевые компоненты HT и VHT, вместе со знаниями, необходимыми для правильной подготовки к экзамену CWNA.

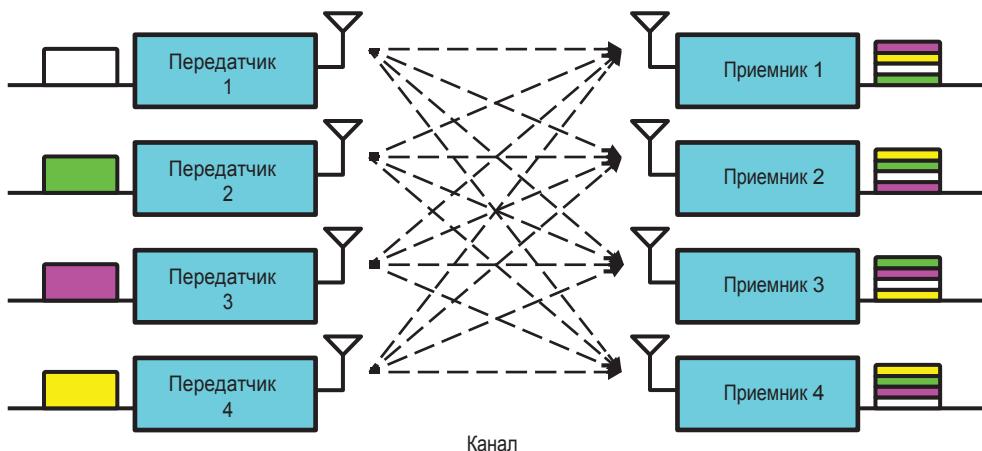
# MIMO

Сердце и душа поправок 802.11n и 802.11ac находятся в Физическом уровне [Physical (PHY) layer], с использованием технологии, называемой много вводов, много выводов [multiple-input, multiple-output (MIMO)]. MIMO требует использование нескольких радиомодулей и антенн, называемых *радиотехническими цепями* [*radio chains*], которые определены позднее в этой главе. Радиомодули MIMO передают несколько радиосигналов в одно и то же время, чтобы воспользоваться преимуществом многолучевого распространения.

В ранних средах 802.11, явление многолучевого распространения (многолучевости) долго вызывало проблемы. *Многолучевое распространение [Multipath]* - это явление распространения, результатом которого является один или более путей одного и того же сигнала, прибывающего на приемную антенну в одно и то же время или в пределах нескольких наносекунд друг от друга. Из-за естественного расширения волн будет проявляться разное поведение распространения: отражение [reflection], рассеяние [scattering], дифракция [diffraction] и преломление [refraction]. Сигнал может отразиться от объекта, или может рассеяться, преломиться или дифрагировать. Эти поведения распространения могут привести в результате к нескольким путям одного и того же сигнала. Как вы узнали из Главы 3 "Основы Радиотехники", негативные эффекты многолучевого распространения могут включать затухание амплитуды и повреждение данных. Системы MIMO, однако, используют преимущества многолучевого распространения. В отличие от радиомодуля один-ввод, один вывод (SISO), который посыпает только один сигнал, радиомодуль MIMO посыпает несколько радиосигналов в зависимости от количества передатчиков, называемых радиотехническими цепями. Не перепутайте несколько радиосигналов, отправленных радиомодулем MIMO с многолучевым распространением [multipath].

В типовых средах внутри помещений, несколько радиосигналов, отправленных радиомодулем MIMO, каждый пройдет несколькими путями, чтобы достичь приемников MIMO. Например, как показано на Рисунке 10.1, на принимающей стороне, радиомодуль MIMO будет слушать всеми антеннами входящие передачи, которые являются несколькими путями прохождения нескольких сигналов от передатчика MIMO. Приемник MIMO затем будет использовать продвинутые методы *цифровой обработки сигналов* [*digital signal processing (DSP)*], чтобы выделить исходные переданные сигналы. Среда с высокой многолучевостью в действительности помогает приемнику MIMO проводить различия между уникальными потоками данных переносимых несколькими радиосигналами. Фактически, если несколько сигналов, отправленных передатчиком MIMO, все придут одновременно на приемник, то сигналы могут погасить друг друга, и производительность, в основном, будет такой же, как и у не-MIMO систем.

**РИСУНОК 10.1** Работа и многолучевое распространение MIMO



Метод передачи нескольких потоков данных, называемом *пространственное мультиплексирование* [*spatial multiplexing (SM)*], предоставляет большую пропускную способность и использует преимущества многолучевого распространения. Системы MIMO могут также использовать несколько антенн для обеспечения лучшего разнесения по передаче и приему, что может увеличить дальность и надежность. Существуют различные способы разнесения по передаче и по приему.

Пространственно-временное блочное кодирование [*Space-time block coding (STBC)*] и разнесение с циклическим сдвигом [*cyclic shift diversity (CSD)*] являются методами разнесения по передаче, где одна и та же передача данных отправляется несколькими антеннами. Связь с STBC возможна только между устройствами MIMO. Сигналы, разнесенные по передаче с CSD могут быть приняты или MIMO или SISO устройствами.

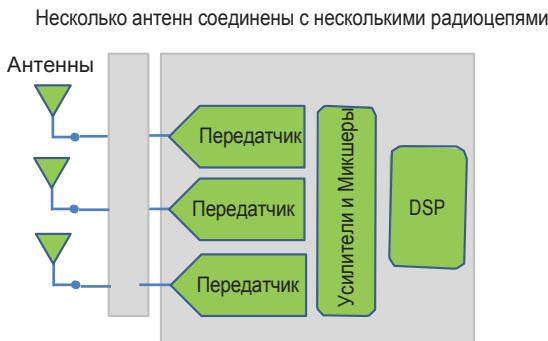
Формирование луча по передаче [*Transmit beamforming (TxBF)*] это способ, когда один и тот же сигнал передается через несколько антенн, и антенны действуют как фазированная решетка. Комбинация Максимального Отношения [*Maximal ratio combining (MRC)*] - это тип техники разнесения по приему, когда несколько принятых сигналов комбинируются, таким образом улучшая чувствительность. Пространственное мультиплексирование и все техники MIMO разнесения по приему и передаче объясняны более детально в следующих разделах.

## Радиотехнические Цепи

Старые радиомодули 802.11 передавали и принимали радиосигналы используя систему один-ввод, один-выход [*single-input, single-output (SISO)*]. Системы SISO используют одну радиотехническую цепь. *Радиотехническая цепь [radio chain]* определена как один радиомодуль (приемопередатчик) и вся его поддерживающая архитектура, включая микшеры, усилители, аналоговые преобразователи, и обработчики цифровых сигналов (DSP).

Как показано на Рисунке 10.2, система MIMO состоит из нескольких радиоцепей, где каждая радиотехническая цепь имеет свою антенну. Система MIMO характеризуется количеством передатчиков и приемников, используемых несколькими радиоцепями. Например, система MIMO  $2 \times 3$  будет состоять из трех радиоцепей с двумя передатчиками и тремя приемниками. Системы MIMO  $3 \times 3$  будут использовать три радиоцепи с тремя передатчиками и тремя приемниками. В системе MIMO первое число всегда относится к передатчикам (TX), а второе число относится к приемникам (RX).

**РИСУНОК 10.2** Радиотехнические цепи MIMO

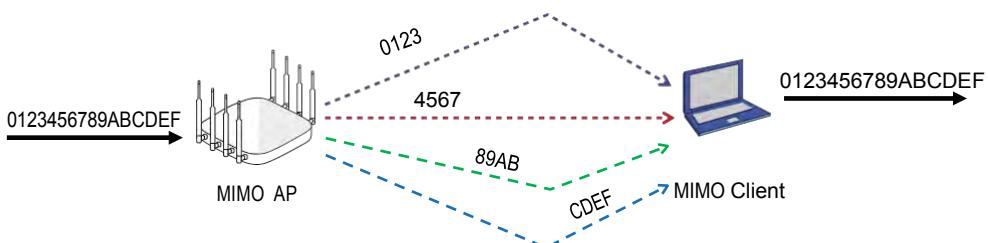


Использование нескольких передатчиков в системе MIMO обеспечивает передачу большего количества данных через пространственное мультиплексирование. Использование нескольких приемников увеличивает отношение сигнал-шум (SNR) за счет продвинутого разнесения антенн MIMO. Оба эти преимущества обсуждаются более детально в следующих разделах. Стандарт 802.11n допускает системы MIMO вплоть до  $4 \times 4$ , использующих четыре радиоцепи. Каждая радиоцепь требует энергию. Система MIMO  $2 \times 2$  будет требовать намного меньше энергии, чем система MIMO  $4 \times 4$ . Радиомодули 802.11n могут иметь вплоть до четырех радиоцепей, а радиомодули 802.11ac точек доступа могут иметь вплоть до восьми радиоцепей.

## Пространственное Мультиплексирование

Вы уже узнали, что радиомодули MIMO передают несколько сигналов. Как показано на Рисунке 10.3, у радиомодуля MIMO также есть способность отправлять независимые уникальные потоки данных. Каждый независимый поток данных называется *пространственный поток [spatial stream]*, и каждый уникальный поток может содержать данные, которые отличаются от других потоков, переданных одной или более другими радиоцепями. Каждый поток также будет идти разными путями, так как существует пространство, как минимум, в половину длины волны между несколькими передающими антеннами. Факт того, что несколько потоков следуют разными путями к приемнику из-за пространства между передающими антennами, называется *пространственное разнесение [spatial diversity]*. Отправка нескольких независимых потоков уникальных данных с использованием пространственного разнесения [spatial diversity] часто называется *пространственное мультиплексирование [spatial multiplexing (SM)]* или *пространственно разнесенное мультиплексирование [spatial diversity multiplexing (SDM)]*. Пространственное мультиплексирование является типом разнесения передачи MIMO и оно требует наличие радиомодулей MIMO на обеих сторонах: на передаче и на приеме.

**РИСУНОК 10.3** Несколько пространственных потоков



Выгода от отправки нескольких уникальных потоков данных в том, что пропускная способность радикально увеличивается, потому что больше данных модулируется. Если точка доступа MIMO посыпает два уникальных потока данных клиентской станции MIMO, которая получает оба потока, пропускная способность фактически удваивается. Если точка доступа MIMO посыпает три уникальных потока данных клиентской станции MIMO, которая принимает все три потока, то пропускная способность фактически утраивается. Как проиллюстрировано на Рисунке 10.3, если точка доступа MIMO посыпает четыре уникальных потока данных клиентской станции MIMO, которая получает все четыре потока, пропускная способность, фактически, становится в четыре раза больше.

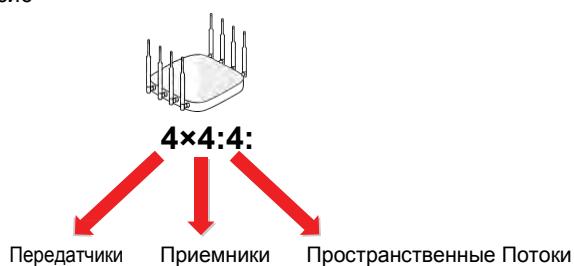
Не перепутайте независимые уникальные потоки данных с количеством передатчиков. В действительности, когда указываете радиомодули MIMO, важно также указывать сколько уникальных потоков данных передается и принимается радиомодулями MIMO. Как показано на Рисунке 10.4, большинство производителей Wi-Fi используют трех-цифровой синтаксис при описании возможностей радиомодулей MIMO.

В системе MIMO, первое число всегда указывает передатчики (TX), а второе число указывает приемники (RX). Третье число представляет сколько уникальных потоков данных может быть отправлено или получено. Например, система MIMO  $4 \times 4:3$  будет использовать четыре передатчика и четыре приемника, но только три уникальных потока данных. Система MIMO  $4 \times 4:4$  будет использовать четыре передатчика и четыре приемника с четырьмя уникальными потоками данных.

#### РИСУНОК 10.4

##### Синтаксис

MIMO



Важно понимать, как радиомодули MIMO используют свои возможности по передаче и по приему. На верхнем уровне вам стоит понимать, что все радиотехнические цепи используются и для передачи, и для приема. Например, ТД  $4 \times 4:4$  всегда использует все четыре радиомодуля при передаче, но в зависимости от различных переменных, только один или два независимых потока данных могут быть переданы по четырем радиоцепям.

Например, если присутствуют хорошие радиоусловия, когда точка доступа  $3 \times 3:3$  и клиентское устройство  $3 \times 3:3$  взаимодействуют друг с другом, три пространственных потока могут быть использованы для однонаправленной (unicast) передачи между ними. Однако, очень часто, из-за изменяющихся радиоусловий, теже самые ТД и клиент могут сдвинуться вниз и передавать только два пространственных потока, используя все три радиоцепи. Радиомодуль MIMO всегда использует антенны и радиоцепи для получения входящих передач.

Когда осуществляется связь с клиентом  $2 \times 2:2$ , ТД  $4 \times 4:4$  будет использовать все четыре радиоцепи для обоих Tx/Rx; однако, максимальное число независимых пространственных потоков, которое может быть модулировано – 2, из-за ограничений клиента  $2 \times 2:2$ . То же самое верно, когда устаревшие радиомодули SISO присутствуют в Wi-Fi среде.

Рдиомодуль MIMO  $4 \times 4:4$  ТД 802.11n будет модулировать только один поток данных при обмене кадрами данных с радиомодулем MIMO  $1 \times 1:1$  клиента 802.11a/b/g. ТД, однако, будет использовать все четыре радиоцепи для модуляции одного потока данных, используя разнесение циклического сдвига (обсуждается позже в этой главе). Дополнительно, так как клиентские устройства большинства Wi-Fi доменов представляют собой смесь из более новых MIMO клиентов и устаревших SISO клиентов, ТД нужно будет модулировать кадры управления и контроля, используя только один пространственный поток.

Также важно понимать, что радиомодули 802.11n/ac имеют много комбинаций возможностей MIMO. Хотя поправка 802.11n определяла использование MIMO систем вплоть до  $4 \times 4:4$ , точки доступа 802.11n высокого класса уровня предприятия были двухдиапазонные ТД  $3 \times 3:3$ .

Однако, большое количество точек доступа 802.11n были двух-диапазонные  $2\times2:2$  ТД из-за низкой цены. Хотя поправка 802.11ac определяла возможность ТД  $8\times8:8$ , они никогда не производились ни одним производителем БЛВС. Вы узнаете в Главе 19, что ТД 802.11ax  $8\times8:8$  теперь являются реальностью. Точки доступа 802.11ac высшего класса используют радиомодуль MIMO  $4\times4:4$ . ТД 802.11ac также производились в обоих форм-факторах  $3\times3:3$  и  $2\times2:2$ . Также, помните, что 802.11ac это только 5ГГц PHY, следовательно, радиомодули 2,4ГГц в ТД 802.11ac все еще используют технологию 802.11n. Например, двух-диапазонная ТД  $4\times4:4$  использует радиомодуль MIMO  $4\times4:4$  802.11ac для 5 ГГц и радиомодуль MIMO  $4\times4:4$  802.11n для 2,4ГГц.

Разнообразие комбинаций МИМО такое же как и различие для клиентских радиомодулей 802.11n/ac. Например, первое поколение смартфонов и планшетов 802.11n использовало радиомодуль  $1\times1:1$ , который фактически работал как радиомодуль SISO с некоторой функциональностью 802.11n PHY/MAC. Радиомодуль  $1\times1:1$  не предлагает всех преимуществ использования пространственных потоков; однако, некоторые из других усовершенствований 802.11n PHY и MAC все же применяется в полосе частот 2,4ГГц. На текущий момент, много устройств IoT передают только в полосе 2,4ГГц, используя технологию 802.11n с радиомодулем  $1\times1:1$ . Использование нескольких цепей в дешевых IoT устройствах обычно является не практичным по причинам экономии заряда батареи или аккумулятора. Рисунок 10.5 представляет широкое разнообразие возможностей МИМО для ТД и клиентских устройств.

**РИСУНОК 10.5** Разнообразие возможностей MIMO



Некоторые ноутбуки высокого-класса с 802.11n/ac имеют возможности MIMO  $4\times4:4$ , но это скорее исключение из нормы. Почти все ноутбуки 802.11n/ac/ax используют MIMO радиомодули или  $3\times3:3$  или  $2\times2:2$ . В сегодняшнем мире, число мобильных устройств Wi-Fi далеко превышает число ноутбуков. Почти все современные смартфоны и планшеты используют радиомодули  $2\times2:2$ . Свыше 70 процентов клиентских устройств MIMO используют радиомодули  $2\times2:2$ . Как ранее упоминалось, основная часть IoT устройств используют только радиомодули MIMO  $1\times1:1$ . Итого, IoT устройства обычно используют радиомодули MIMO  $1\times1:1$ , а мобильные устройства используют радиомодули MIMO  $2\times2:2$ , из-за того, что дополнительные радиоцепи будут уменьшать заряд батареи устройств слишком быстро.

Клиенты и ТД могут договариваться друг с другом относительно своих возможностей MIMO, используя информационные элементы HT/VHT внутри кадров управления. Например,

ТД 4×4:4 будет вещать на всех (broadcast) в кадре маяке все возможности MIMO ТД. А клиент MIMO 2×2:2 будет использовать зондирующие запросы и запросы на ассоциацию. Когда клиентский радиомодуль присоединяется к базовому составу сервиса (BSS), точка доступа уведомляется о MIMO возможностях клиентского радиомодуля.

## Сравнение разнесений MIMO и SISO

Если вы закроете одно ухо рукой, будете ли вы слышать одним ухом лучше или хуже? Очевидно, вы будете слышать лучше двумя ушами. Думаете ли вы, что будете способны слышать более четко, если бы у вас было три или четыре уха вместо двух? Думаете ли вы, что будете способны слышать звуки на гораздо большем расстоянии, если бы у вас было три или четыре уха вместо двух? Да, человек слышал бы более четко и на большее расстояние, если бы был оснащен еще двумя ушами. В системах MIMO применяются расширенные возможности разнесения антенн, что является аналогом с наличием нескольких ушей.

Разнесение антенн часто является ошибочным для возможностей пространственного мультиплексирования, которое используется MIMO. Разнесение антенн (и приема и передачи) – это способ использования нескольких антенн, чтобы выдержать негативные воздействия многолучевого распространения [multipath]. Как вы уже знаете, MIMO использует преимущество многолучевого распространения [multipath] с пространственным мультиплексированием, чтобы увеличить пропускную способность данных. Простое разнесение антенн [*antenna diversity*] – это метод компенсации многолучевого распространения, в отличие от использования многолучевого распространения. Многолучевое распространение производит несколько копий одного и того же сигнала, который прибывает на приемник в разное время с разными амплитудами.

В Главе 5 “Радиосигналы и Концепции Антенн” вы узнали о традиционном разнесении антенн, которое состоит из одного радиомодуля с двумя антенными. Большинство радиомодулей SISO используют *переключаемое (или коммутируемое) разнесение [switched diversity]*. Когда принимается радиосигнал, системы с переключаемым разнесением слушают несколькими антennами. Несколько копий одного и того же сигнала прибывают на приемные антенны с разными амплитудами. Выбирается сигнал с лучшей амплитудой, а другие сигналы игнорируются. Переключаемое разнесение также используется при передаче, но используется только одна антenna. Передатчик будет передавать через antennу, через которую был слышен сигнал с лучшей амплитудой последний раз.

По мере увеличения расстояния между передатчиком и приемником, амплитуда принимаемого сигнала уменьшается до уровня близкого к уровню шума. По мере уменьшения отношения сигнал-шум(SNR), растет вероятность повреждения данных. Прослушивание двумя антеннами увеличивает вероятность услышать, по крайней мере, один сигнал без поврежденных данных. Теперь представьте, если бы у вас было три или четыре антены слушающих, чтобы услышать лучший принимаемый сигнал, используя переключаемое разнесение. Вероятностные шансы услышать сигналы с более сильными амплитудами и неповрежденными данными увеличились бы еще больше. Повышенная вероятность услышать хотя бы один неискаженный сигнал в системе с переключаемым разнесением, использующей три или четыре антены, часто приводит к увеличению дальности действия.

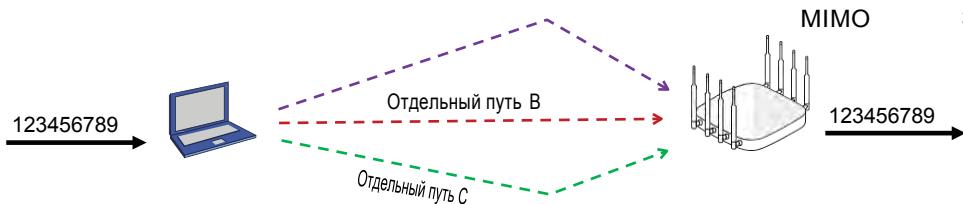
## Комбинация Максимального Отношения

Когда используется разнесение по приему в MIMO, сигналы могут быть также линейно сложены с использованием метода цифровой обработки сигнала, называемой *комбинация максимального отношения [maximal ratio combining (MRC)]*. Алгоритмы MRC используются для сложения (комбинирования) нескольких полученных сигналов путем просмотра каждого уникального сигнала и оптимального объединения методом, который является аддитивным, а не деструктивным.

Системы MIMO, использующие MRC, фактически поднимают уровень SNR принимаемого сигнала. Как показано на Рисунке 10.4, комбинация максимального отношения также является полезной, когда старые радиомодули SISO передают приемнику MIMO и происходит многолучевое распространение [multipath]. На Рисунке 10.6, три различных пути одного и того же сигнала SISO приходят на MIMO приемник. Алгоритм MRC фокусируется на сигнале с самым высоким уровнем SNR; однако, он может объединить информацию из более зашумленных сигналов. Конечный результат - это то, что случается меньше повреждения данных, потому что восстанавливается более точная оценка исходных данных.

**РИСУНОК 10.6**      Комбинация максимального отношения





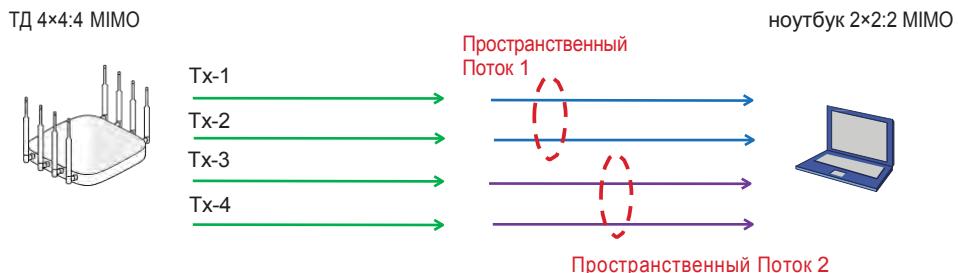
MRC использует функцию комбинации по приему, которая оценивает фазу и SNR каждого входящего сигнала. Каждый принятый сигнал со сдвигом фазы, так что они могут быть объединены (комбинированы). Амплитуда входящего сигнала также модифицируется, чтобы сфокусироваться на сигнале с лучшим SNR.

## Пространственно-Временное Блочное Кодирование

Ранее в этой главе мы обсуждали пространственное мультиплексирование, которое является одним типом разнесения передачи MIMO. *Пространственно-временное блочное кодирование [Space-time block coding (STBC)]* - это метод, где одна и та же информация передается по двум и более антеннам; однако, количество антенн должно быть четным. STBC - это другой тип разнесения передачи MIMO. STBC может быть использован, когда количество радиоцепей превышает количество пространственных потоков. Отправка нескольких копий одной и той же информации по нескольким антеннам не увеличивает реальную скорость передачи данных при добавлении передающих антенн. Однако, STBC увеличивает способность приемника детектировать сигналы при более низком SNR, чем это было бы возможно в противном случае. Приемная чувствительность радиосистемы улучшается. STBC и разнесение с циклическим сдвигом [cyclic shift diversity (CSD)] техника разнесения передачи, где те же самые передаваемые данные отправляются через несколько антенн. Связь STBC возможна только между MIMO устройствами. Сигналы с разнесением могут быть приняты или MIMO, или устаревшими SISO устройствами.

Рисунок 10.7 дает визуализацию STBC между устройствами MIMO. ТД 4x4:4 может использовать STBC для передачи двух копий пространственного потока #1 по радиомодулям TX-1 и TX-2. Дополнительно, две копии пространственного потока #2 предаются по радиомодулям TX-3 и TX-4. Клиент MIMO 2x2:2 затем использует STBC чтобы декодировать оба потока. Так как несколько копий обоих потоков было отправлено ТД, вероятность успешной доставки неповрежденных данных намного лучше.

**РИСУНОК 10.7** Пространственно временное блочное кодирование



## Разнесение с Циклическим Сдвигом

*Разнесение с циклическим сдвигом [Cyclic shift diversity (CSD)]* - это другой способ разнесения по передаче, установленный в радиомодулях MIMO 802.11n и 802.11ac. В отличии от STBC, сигнал от передатчика, который использует CSD, может быть принят устаревшими 802.11b/g и 802.11a SISO устройствами. Для смешанных установок, где 802.11n/ac сосуществует с 802.11b/g и 802.11a устройствами, необходимо иметь способ передачи символов в старой преамбуле OFDM по нескольким передающим антеннам. К каждому переданному сигналу применяется циклическая задержка и используется CSD. Задержка вычисляется таким образом, чтобы минимизировать корреляцию между несколькими сигналами. Обычная устаревшая система будет трактовать несколько принятых сигналов как версии многолучевого распространения одного и того же сигнала. Циклическая задержка выбирается так, чтобы быть в пределах защитного интервала [guard interval (GI)] так, чтобы это не вызвало избыточной межсимвольной интерференции (ISI). Система МИМО без проблем использует несколько сигналов для улучшения общего SNR преамбулы. Подробности того как работает CSD не являются частью экзамена CWNA. CSD - одна из уточненных и наименее обсуждаемых характеристик 802.11n/ac, но тем не менее она все же важна для радиоинженеров производителей оборудования.

## Формирование Луча Передачи

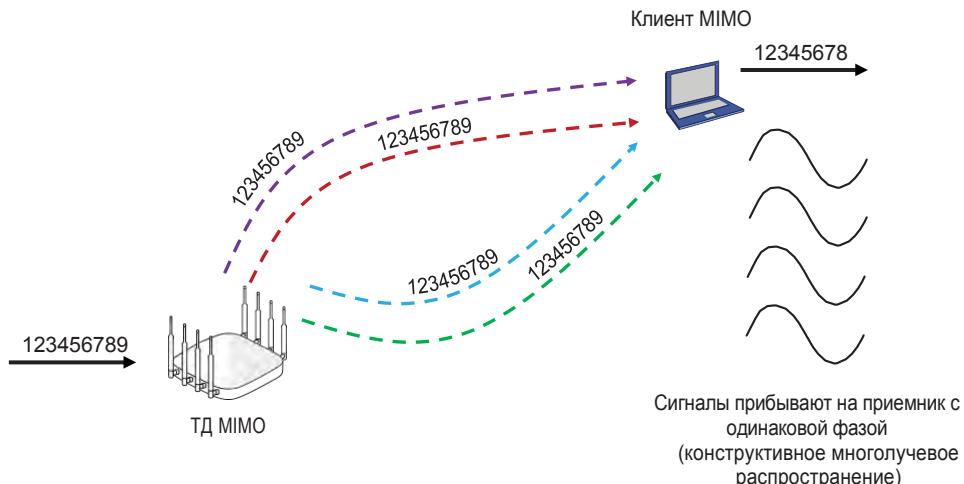
Поправка 802.11n предложила опциональную возможность для физического уровня [PHY], названную *формирование луча передачи [transmit beamforming (TxBF)]*, которая использует подстройку фазы. Формирование луча передачи может быть использовано, когда количество передающих антенн больше чем пространственных потоков.

Формирование луча передачи - это метод, который позволяет передатчикам МИМО, использующим несколько антенн, настраивать фазу и амплитуду исходящих передач согласованным способом. Когда несколько копий одного и того же сигнала отправлены получателю, сигналы обычно прибывают с разными друг от друга фазами. Если передатчик (TX) знает о радио характеристиках местоположения приемника, то фаза нескольких сигналов, отправляемых передатчиком MIMO может быть подстроена. Когда несколько сигналов прибывает на приемник, и они в фазе, это приводит в результате к конструктивному многолучевому распространению вместо деструктивного многолучевого распространения, вызванного сигналами не в фазе. Тщательный контроль фаз сигналов, передаваемых через несколько антенн, имеет эффект эмуляции направленной антенны.

Так как формирование луча по передаче приводит к конструктивному многолучевому распространению, то в результате получаем более высокое соотношение сигнал-шум и более высокую принимаемую амплитуду. Следовательно, формирование луча по передаче [transmit beamforming] приведет к большему расстоянию обслуживания для индивидуальных клиентов, взаимодействующих с точкой доступа. Формирование луча по передаче также приведет к большей пропускной способности из-за большего SNR, которой позволит использовать более сложные методы модуляции, которые смогут кодировать больше битов данных. Более высокий SNR также приведет к меньшим повторным передачам на уровне 2.

Формирование луча по передаче может быть использовано вместе с пространственным мультиплексированием (SM); однако, число пространственных потоков ограничены числом приемных антенн. Например, радиомодуль ТД MIMO  $4 \times 4:4$  может передавать клиентскому радиомодулю MIMO  $2 \times 2:2$ , который может принимать только два пространственных потока. Радиомодуль MIMO  $4 \times 4:4$  отправит только два пространственных потока, но может также использовать другие антенны для формирования луча передачи. Однако, как показано на Рисунке 10.8, при использовании формирования лучом по передаче, передатчик обычно не посыпает несколько уникальных пространственных потоков, но вместо этого посыпает несколько копий того же самого потока данных с фазой, подстроенной для каждого радиосигнала.

**Р И С У Н О К 1 0 . 8**      Формирование луча[beamforming] по передаче данных



Передатчики, которые используют формирование луча будут пытаться настроить фазу сигналов на основе обратной связи от приемников путем использования *исследующих кадров [sounding frames]*. Передатчик считается *формирователем луча [beamformer]*, а приемник считается *получателем луча [beamformee]*. Формирователь луча [beamformer] и получатель луча [beamformee] работают вместе, чтобы сообщить друг другу о характеристиках канала МИМО. Этот обмен исследующих кадров используется, чтобы измерить радиоканал и создать вычислительную оценку как лучше направить радиоволновую энергию к приемнику. Оценка называется *управляющая матрица [steering matrix]*.

Формирование луча передачи полагается на *неявную обратную связь [implicit feedback]* или  *явную обратную связь [explicit feedback]* от передатчика и приемника. Любой кадр может использоваться как исследующий кадр [sounding frame]. Кадры данных с пустой [null] функцией могут быть использованы, если другие кадры не используются.

Когда используется неявная обратная связь, формирователь луча [beamformer] посыпает зондирующие [sounding] кадры и затем получает длинные тренировочные символы, переданные получателем луча [beamformee], которые позволяют каналу МИМО между получателем луча [beamformee] и формирователем луча [beamformer] быть оцененным формирователем луча [beamformer]. Другими словами, нет прямой обратной связи от получателя луча [beamformee], и таким образом формирователь луча [beamformer] создает управляющую матрицу. Хорошой аналогией для неявной обратной связи является гидролокация [sonar]. Гидролокация - это метод, в котором подводные лодки используют распространение звука под водой для обнаружения других судов. Подводные лодки посыпают звуковую волну, и на основе характеристик возвращившейся звуковой волны, экипаж может определить тип судна, который может быть на пути подводной лодки. При этом, нет прямой явной обратной связи от судна к подводной лодке.

Намного больше информации может быть передано в обе стороны между двумя радиомодулями МИМО, если оба они поддерживают явную обратную связь [explicit feedback]. Когда используется явная обратная связь, получатель луча [beamformee] производит прямую оценку канала по тренировочным символам, отправленными формирователем луча [beamformer]. Получатель луча [beamformee] берет эту информацию и посыпает дополнительную обратную связь обратно формирователю луча [beamformer]. Другими словами, получатель луча [beamformee] создает управляющую матрицу [steering matrix]. Формирователь луча затем передает, на основе обратной связи от получателя луча [beamformee]. Стоит отметить, что явное формирование луча никогда не было принято производителями БЛВС для радиомодулей 802.11n.

Один производитель БЛВС внедрил некоторые возможности неявного формирования луча в некоторых своих ТД 802.11n. Поправка 802.11ac определяет только явное формирование луча, а производители БЛВС встроили эту возможность в радиомодули 802.11ac и 802.11ax. Явное формирование луча, которое используется в 802.11ac и 802.11ax, объяснено в следующем разделе.

## Явное Формирование Луча

В этом разделе вы узнаете о явном формировании луча, которое используется радиомодулями 802.11ac и 802.11ax, и как оно используется с многопользовательским МИМО [multi-user MIMO (MU-MIMO)]. Чтобы произвести формирование луча, несколько радиоцепей в ТД передают одну и ту же информацию через разные антенны. ТД выставляет время их передач так, чтобы волны со всех антенн пришли на принимающий радиомодуль в одно и то же время и в одной фазе друг с другом. Это должно привести к увеличению сигнала

примерно на 3 децибела. Это увеличение в силе сигнала может сдвинуть связь между радиомодулями на более высокую скорость передачи данных. Этого увеличения недостаточно, чтобы повлиять на высокие 256-QAM скорости передачи данных (или низкие скорости передачи данных), но оно влияет на связь на средние скорости передачи данных.

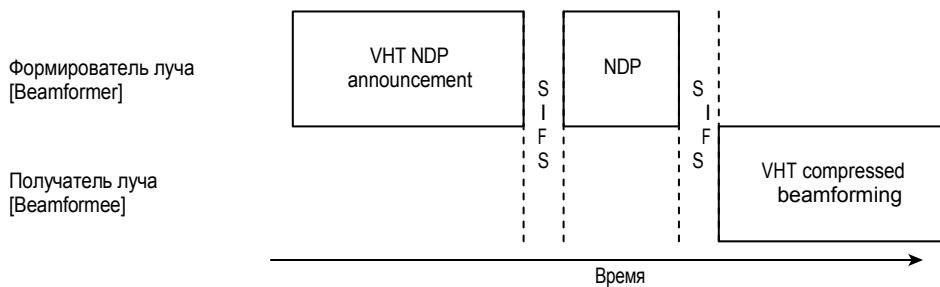
Явное формирование луча требует поддержку и передатчиком (формирователем луча[beamformer]) и приемником (получателем луча[beamformee]) для того, чтобы использовать формирование луча. Явное формирование луча использует интерактивный процесс калибровки, чтобы идентифицировать как произвести передачу с использованием нескольких радиоцепей. Этот процесс называется *исследованием канала [channel sounding]*.

Чтобы начать процесс, формирователь луча [beamformer] передает кадр оповещения с пустым пакетом данных [null data packet (NDP) announcement frame], который оповещает получателя луча [beamformee] о намерении отправить передачу со сформированным лучом.

Затем за этим следует формирователь луча [beamformer] с кадром NDP. Получатель луча [beamformee] обрабатывает каждую OFDM поднесущую и создает информацию для обратной связи. Обратная связь содержит информацию относительно мощности и фазового сдвига каждой пары, передающей и принимающей антенн. Эта информация используется для создания матрицы обратной связи [feedback matrix], которая затем сжимается и отправляется обратно формирователю луча [beamformer]. Рисунок 10.9 показывает этот обмен кадров.

Формирователь луча [beamformer] использует матрицу обратной связи [feedback matrix] для вычисления управляющей матрицы [steering matrix], которая используется для направления передачи данных на получателя луча [beamformee].

**Р И С У Н О К 1 0 . 9**      Процесс исследования однопользовательского формирования луча



Хотя этот раздел объясняет процесс формирования луча, в действительности он объясняет то, что называется *однопользовательское формирование луча [single-user beamforming]*. Следующий раздел познакомит вас с многопользовательским MIMO [multi-user MIMO (MU-MIMO)]. После объяснения MU-MIMO, мы продолжим дальше объяснять формирование луча, особенно много-пользовательского формирования луча [multi-user beamforming].

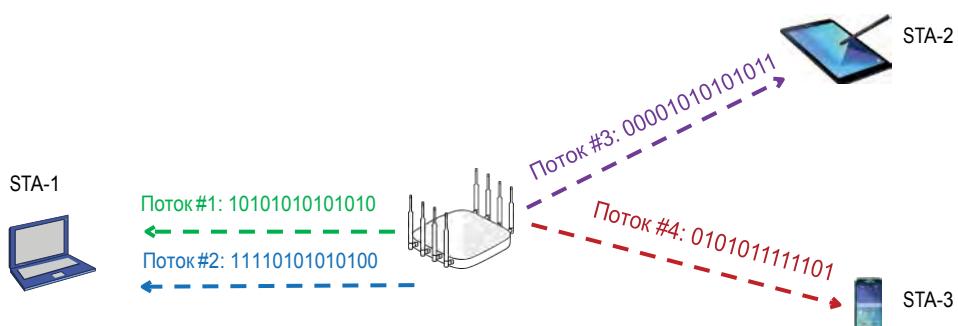
## Многопользовательское MIMO

До 802.11ac, ТД 802.11n были способны поддерживать связь только с одним устройством одновременно. Когда ТД осуществляла передачу, она была адресована одному клиентскому устройству. С 802.11ac, стало возможным ТД 802.11ac поддерживать связь до четырех устройств одновременно, используя технологию MU-MIMO. Термин многопользовательский [*multi-user (MU)*] просто означает, что передачи между ТД и несколькими клиентами может происходить в одно и то же время, в зависимости от поддерживаемой технологии. MU-MIMO разрешает нисходящую [*downlink*] связь нескольким пользователям от точки доступа [ТД] во время одной и той же возможности передачи [*transmission opportunity (TXOP)*]. MU-MIMO использует преимущество того факта, что ТД имеют несколько радиомодулей и антенн. Точка доступа MU-MIMO передает уникальные модулированные потоки данных нескольким клиентам одновременно. Цель – это улучшить эффективность путем использования меньшего эфирного времени.

Однако, не все радиомодули 802.11ac поддерживают MU-MIMO, поддерживая только однопользовательскую связь MIMO. Дополнительно, радиомодули 802.11n поддерживают только однопользовательскую связь MIMO и не поддерживают MU-MIMO. Чтобы отличать стандарт технологии MIMO, которая была представлена в 802.11n от MU-MIMO, мы будем называть ее *однопользовательское MIMO (SU-MIMO)*.

Цель MU-MIMO – использовать как можно больше пространственных потоков, ведется ли передача с одним клиентом с использованием четырех пространственных потоков, или с четырьмя клиентами с использованием одного пространственного потока каждому. MU-MIMO поддерживается только для нисходящей [*downlink*] передачи от ТД 802.11ac к клиентам 802.11ac. Рисунок 10.10 показывает ТД, которая способна передавать четыре пространственных нисходящих [*downlink*] потока. В этой иллюстрации, ТД использует два пространственных потока для передачи к ноутбуку, третий поток для передачи к планшету, четвертый поток для передачи к смартфону.

**РИСУНОК 10.10** Многопользовательское MIMO



Как показано на Рисунке 10.11 пятичисленный синтаксис иногда используется при описании возможностей радиомодуля MU-MIMO. В системе MU-MIMO, первое число всегда относится к передатчикам (TX), второе число относится к приемникам (RX). Третье число представляет сколько уникальных однопользовательских [*single-user (SU)*] потоков данных может быть отправлено или принято. Четвертое число обозначает сколько многопользовательских (MU) потоков может быть передано. Пятое число используется для представления группы MU-MIMO или сколько клиентов MU-MIMO

может принимать передачи одновременно. Например, ТД 802.11ac 4×4:4:3:3 может передавать до четырех пространственных потоков к одному пользователю при работе в режиме SU-MIMO. Однако, только три пространственных потока могут быть использованы для передач MU-MIMO к, максимум, трем MU-MIMO клиентам, с каждым клиентом, принимающим один поток. Если ТД 802.11ac работает как ТД MU-MIMO 4×4:4:3:2, только два клиента будут принадлежать группе MU-MIMO. Так как три пространственных потока доступны для MU-MIMO передач, один пространственный поток будет предназначен для одного клиента и два пространственных потока для других клиентов, принадлежащих группе MU-MIMO.

**РИСУНОК 10.11** Синтаксис MU-MIMO



Итак, как будет это работать, если будет 20 MU-MIMO клиентов, ассоциированных с ТД 802.11ac? ТД будет принимать решение, какие клиенты будут принимать нисходящие передачи MU-MIMO, а какие клиенты будут назначены в клиентскую группу MU-MIMO. Например, три клиента могут принять пространственные потоки одновременно в первой нисходящей [downlink] передаче, а затем три других клиента принять пространственные потоки одновременно в следующей нисходящей передаче.

Следует понимать, что передачи MU-MIMO 802.11ac являются только нисходящими. ТД 802.11ac MU-MIMO может передавать нисходящий канал связи [downlink] одному или более клиентам 802.11ac MU-MIMO. MU-MIMO в восходящем канале связи [uplink] пока еще не существует, хотя есть опциональная возможность технологии 802.11ax.

Формирование луча является критичной частью MU-MIMO. Предыдущий раздел этой главы объяснял явное формирование луча. В следующем разделе, мы объясним почему явное формирование луча является необходимым для того, чтобы MU-MIMO работало.

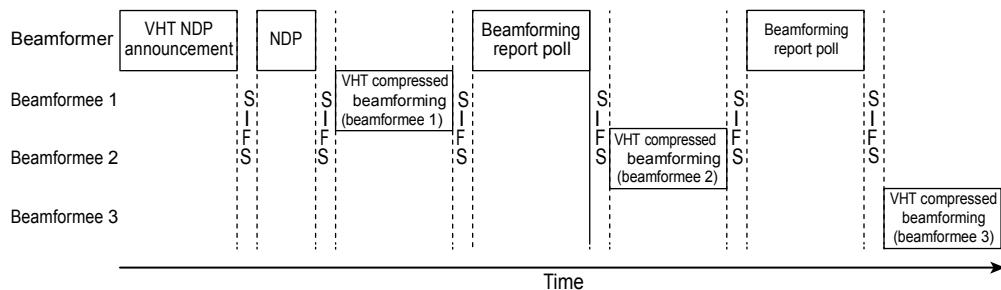
## Многопользовательское Формирование Луча

Ранее в этой главе мы объяснили, как 802.11ac выполняет явное формирование луча. Мы также объяснили принципы MU-MIMO. Сейчас настало время обсудить эти две технологии вместе.

В однопользовательском MIMO [single-user MIMO], формирование луча [beamforming] использует подстройку фазы радиосигнала, чтобы увеличить силу сигнала у клиента – в надежде позволить ТД и клиенту работать с использованием более высоких скоростей передачи. В MU-MIMO, задача формирования луча выполняется не только для передачи одному клиенту; а также выполняется для передачи нескольким клиентам одновременно.

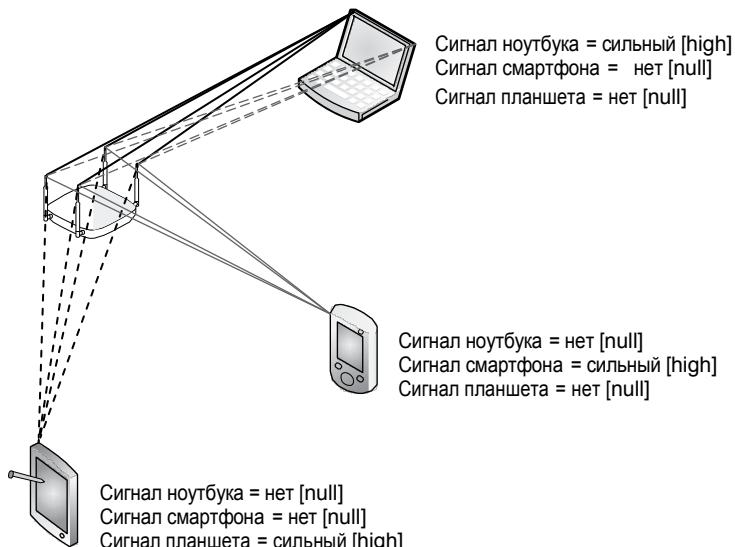
Чтобы начать процесс формирования луча [beamforming] в MU-MIMO, ТД выполняет процедуру исследования канала [sounding channel], похожую, но более сложную, чем в SU-MIMO. Чтобы начать процесс, ТД передает кадр оповещения с пустым пакетом данных [null data packet (NDP) announcement frame], оповещая нескольких получателей луча [beamformees] о намерении отправить передачу со сформированным лучом. Далее за этим следует кадр NDP от ТД. Также как при формировании луча для одного пользователя, каждый получатель луча обрабатывает каждую OFDM поднесущую и создает информацию обратной связи, создавая сжатую матрицу обратной связи [feedback matrix]. Первый получатель луча отвечает ТД своей сжатой матрицей обратной связи. Затем ТД опрашивает каждого дополнительного получателя луча последовательно, используя кадры Опросов Отчета Формирования Луча [Beamforming Report Poll frames]. Рисунок 10.12 иллюстрирует этот процесс.

**РИСУНОК 10.12** Процесс исследования в многопользовательском формировании луча



Затем ТД использует матрицу обратной связи от каждого получателя луча, чтобы создать единую *управляющую матрицу [steering matrix]*. Управляющая матрица определяет параметры передачи для связи между каждой антенной на ТД и каждой антенной на каждом клиентском устройстве, как показано на Рисунке 10.13.

**РИСУНОК 10.13** Передачи сформированного луча в среде MU-MIMO

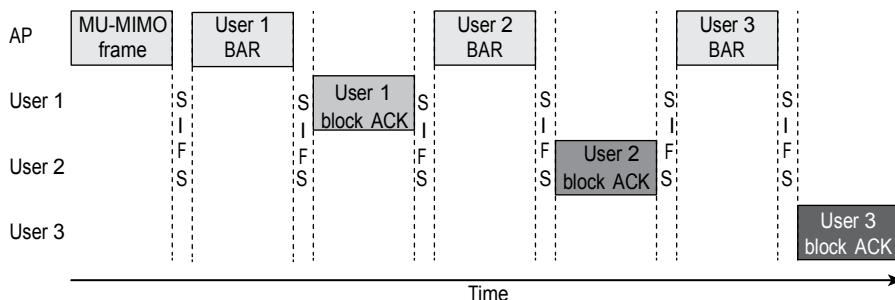


Важно помнить, что на Рисунке 10.13, ТД посылает 16 передач, по 4 с каждой антенны. Из этих 16 передач, приемной антенне нужно уметь выделить и интерпретировать сигнал, который направлен к ней, при этом пытаясь игнорировать другие 12 передач. Сигналы сформированного луча для определенного клиента отправляются по времени, чтобы прибыть в одно и то же время и синхронизованно, фактически создавая более сильный сигнал. Получатели луча [*beamformees*], которые находятся слишком близко друг к другу, могут испытывать межпользовательскую [*inter-user*] интерференцию от сигналов, направленных к другим пользователям. В идеале, пользователи физически достаточно разнесены друг от друга, а сигнал сформированного луча для пред назначенного пользователя является сильным, в то время как сигнал, принимаемый другими пользователями, является слабым. Рисунок 10.3 иллюстрирует как различные сигналы должны распознаваться пользователем. Если пользовательские устройства достаточно разнесены, то сигнал сформированного луча к пред назначенному пользователю должен быть сильным, а сигналы, получаемые другими пользователями, должны *отсутствовать [null]* или быть слабыми.

После того как ТД передаст многопользовательский кадр, каждая клиентская станция должна подтвердить этот кадр. Как утверждалось ранее, MU-MIMO работает только от ТД к клиенту, поэтому подтверждения должны быть однопользовательскими передачами. Так как каждый кадр 802.11ac является кадром A-MPDU, доставка всех индивидуальных MPDU подтверждается Блоковым подтверждением (Block ACK). Когда требуется Block ACK, инициатор кадра, в этом случае - ТД, отправляет кадр *Запрос Блокового Подтверждения*

[*Block Acknowledgment Request (BAR)*] получателю, который отвечает Блоковым подтверждением [Block ACK]. Так как это кадр MU-MIMO, ТД посыпает кадр BAR пользователю, ждет Block ACK от этого пользователя, а затем последовательно повторяет этот процесс с другими пользователями. Рисунок 10.14 иллюстрирует эту последовательность.

**РИСУНОК 10.14** Блоковые подтверждения MU-MIMO



Возможности MU-MIMO в нисходящем канале связи [*downlink*] были введены во втором поколении точек доступа 802.11ac; однако широкое применение технологии MU-MIMO является редкостью. Хотя MU-MIMO звучит грандиозно на бумаге, внедрение в реальном мире является не практической по следующим причинам:

- Существует очень немного клиентов 802.11ac с поддержкой MU-MIMO, и технология редко используется на предприятиях. Клиенты должны также поддерживать явное формирование луча [*explicit beamforming*]. Стоит заметить, что более новые клиенты 802.11ax поддерживают MU-MIMO.
- MU-MIMO требует пространственного разнесения; следовательно, физическое расстояние между клиентами является необходимостью. Большинство сегодняшних установок Wi-Fi на предприятиях включает высокую плотность пользователей, которая не благоприятна для MU-MIMO условий.
- Так как MU-MIMO требует пространственного разнесения, то нужна заметная дистанция между клиентами и ТД. Большинство современных установок Wi-Fi на предприятиях включают высокую плотность пользователей, которая не благоприятна для MU-MIMO условий.
- MU-MIMO требует передачу с формированием луча [*transmit beamforming (TxBF)*], которая требует исследующие кадры [*sounding frames*]. Исследующие кадры добавляют дополнительные накладные расходы [*overhead*], особенно когда большинство кадров данных небольшие. Накладные расходы от исследующих кадров обычно нивелируют любую производительность, полученную от ТД 802.11ac, передающую в нисходящем канале связи [*downlink*] одновременно нескольким клиентам 802.11ac.

Как ранее упоминалось, клиенты 802.11ax поддерживают нисходящую связь MU-MIMO, так что поддержка MU-MIMO со стороны клиентов растет. Поправка 802.11ax также предлагает опционально связь MU-MIMO в восходящем канале связи [*uplink*]. Больше информации можно найти в Главе 19.

# Каналы

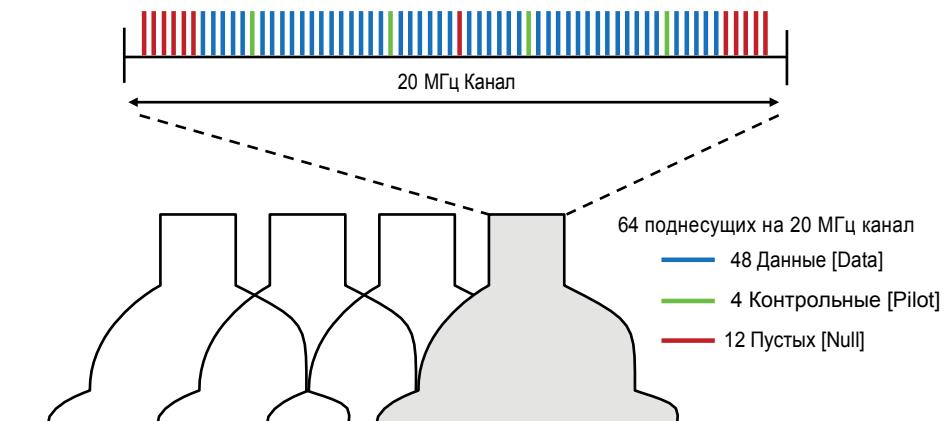
В предыдущих главах вы узнали, что поправка 802.11a определяла способность радиомодулей использовать технологию мультиплексирования с ортогональным частотным разделением [*orthogonal frequency-division multiplexing (OFDM)*] в 5ГГц полосах U-NII. 802.11g определяла возможности радиомодулей, использующих ERP-OFDM, которая, фактически, та же самая технология, кроме того, что передачи осуществляются в полосе 2,4ГГц ISM. Поправка 802.11n также определяет использование OFDM каналов. Однако, для радиомодулей 802.11n (HT) существуют ключевые отличия. Как упоминалось ранее в этой главе, радиомодули 802.11n (HT) могут работать в обоих частотах.

Вы уже знаете, что радиомодули MIMO используют пространственное мультиплексирование, чтобы отправить несколько независимых потоков уникальных данных. Пространственное мультиплексирование является одним из методов увеличения пропускной способности. Каналы OFDM, используемые радиомодулями MIMO, используют больше поднесущих, а также существует опция по объединению каналов вместе. Большая ширина полосы частот, предоставляемая каналами OFDM, используемыми радиомодулями 802.11n (HT) и 802.11ac (VHT), может также обеспечить большую скорость передачи данных и потенциально большую пропускную способность.

## Каналы 20 МГц

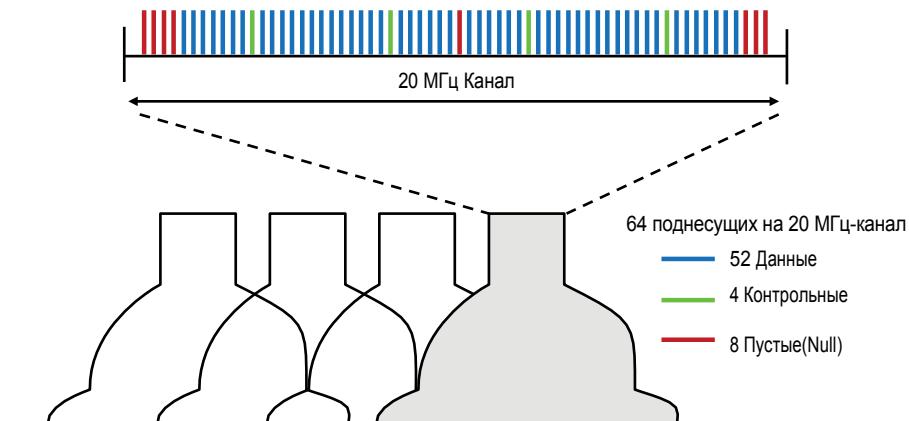
Как вы узнали из Главы 6 “Беспроводные Сети и Технологии Расширения Спектра”, радиомодули 802.11a и 802.11g используют 20МГц OFDM каналы. Как показано на Рисунке 10.5, каждый канал состоит из 64 поднесущих. Сорок восемь поднесущих передают данные, четыре поднесущие используются в качестве контрольных сигналов [pilot tones] для динамической калибровки между передатчиком и приемником. Оставшиеся поднесущие не используются. OFDM технология также применяет использование сверточного кодирования [convolutional coding] и прямое исправление ошибок [forward error correction].

**РИСУНОК 10.15** 20 МГц не-HT [non-HT] (802.11a/g) канал



Радиомодули 802.11n (НТ) и 802.11ac (VHT) также используют ту же самую технологию OFDM. У 20-МГц каналов, используемых радиомодулями НТ и VHT, есть на четыре поднесущих для данных больше, чем у не-НТ OFDM канала. В результате, 20 МГц канал НТ с одним пространственным потоком может обеспечить большую агрегированную пропускную способность для одного и того же частотного пространства. Как показано на Рисунке 10.6, у 20МГц HT/VHT OFDM канала также есть 64 поднесущих. Однако, 52 поднесущих передают данные, а 4 поднесущих используются в качестве контрольных сигналов [pilot tones] для динамической калибровки между передатчиком и приемником. Другими словами, несмотря на то, что то еще есть некоторые неиспользуемые поднесущие, радиомодули НТ или VHT используют на четыре поднесущих больше для передачи данных. Использование этих четырех дополнительных поднесущих является более эффективным использованием доступного частотного пространства в 20 МГц каналах.

**РИСУНОК 10.16** 20 МГц каналы НТ или VHT



## Каналы 40 МГц

У радиомодулей 802.11n и 802.11ac также есть возможность использование 40 МГц OFDM каналов. Как показано на Рисунке 10.17, 40 МГц каналы используют 128 OFDM поднесущих; 108 поднесущих передают данные, а 6 поднесущих используются как контрольные сигналы [pilot tones] для динамической калибровки между передатчиком и приемником. Оставшиеся поднесущие не используются и работают как защитные полосы. 40 МГц канал, фактически, удваивает ширину полосы частот, доступной для передачи данных.

The 40 МГц каналы, используемые радиомодулями НТ и VHT, это, фактически, два 20 МГц канала, которые соединены вместе. Каждый 40 МГц канал состоит из первичного [primary] и вторичного [secondary] 20МГц каналов. Первичный и вторичный 20МГц каналы должны быть соседними 20МГц каналами по частотам, на которых они работают. Как показано на Рисунке 10.18, два 20 МГц канала, используемых для формирования 40МГц канала, обозначены как первичный [primary] и вторичный [secondary], и обозначаются двумя полями в теле определенных кадров управления 802.11.

РИСУНОК 10.17 40 МГц канал HT или VHT

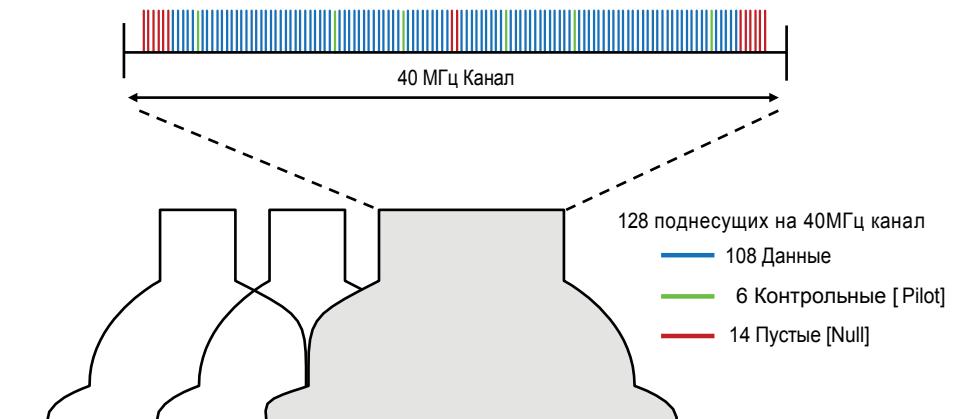
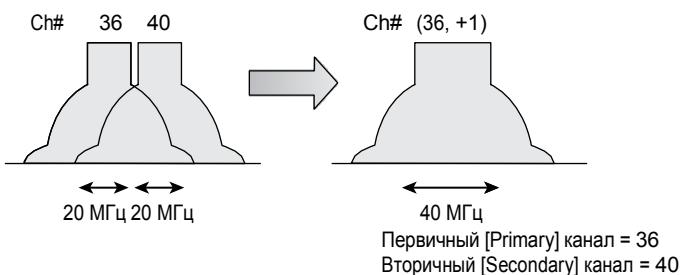


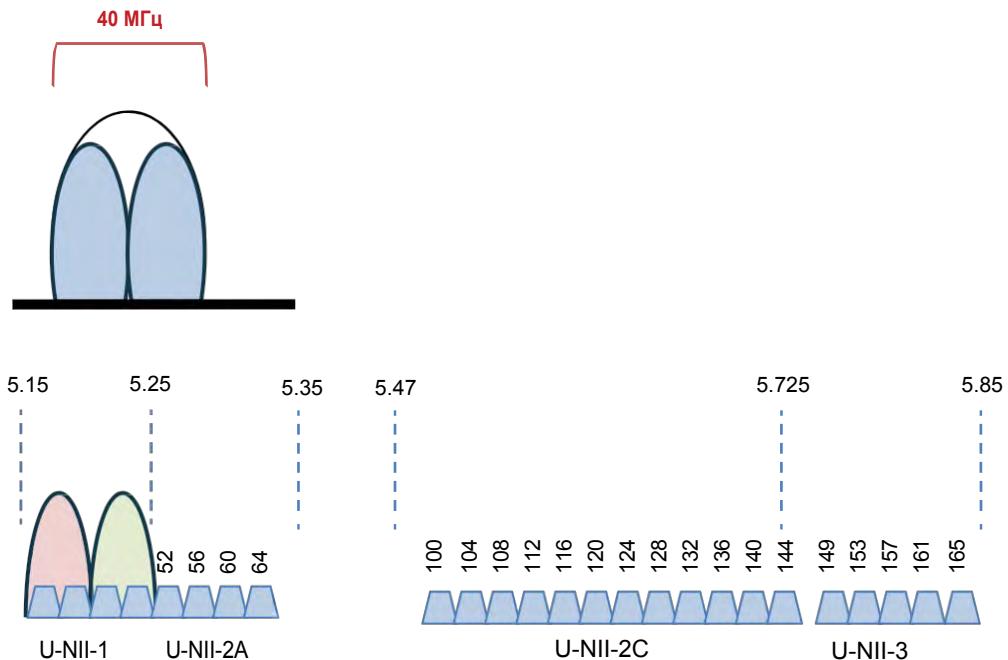
РИСУНОК 10.18 Соединение каналов [Channel bonding]



Первичное поле [primary field] указывает номер первичного канала. В 40МГц каналах в 802.11n положительный или отрицательный сдвиг [offset] указывает - находится ли вторичный канал выше или ниже первичного канала. 802.11ac (VHT) не указывает никакой сдвиг канала [channel offsets], но вместо этого указывает центральную частоту 40МГц канала. Однако, производители БЛС не указывают центральную частоту при настройке 40 МГц канала на точке доступа 802.11ac. Вместо этого, выбирается номер 20 МГц канала, и этот канал работает как первичный канал. Первичный и вторичный каналы используются вместе только для передачи кадров данных между ТД 802.11n/ac и клиентом 802.11n/ac. Для обратной совместимости, все кадры управления и контроля 802.11 передаются только по первичному каналу. Также, только первичный канал используется для передачи между ТД 802.11n/ac и устаревшими клиентами 802.11a/g. Обратите, пожалуйста, внимание, что устройства 802.11ax также поддерживают объединение каналов [channel bonding] вместе с основной массой характеристик, обсуждаемых в этой главе.

Модели переиспользования каналов, использующих 40 МГц каналы на 5 ГГц, являются состоятельными, потому что все ширины полос частот доступны в полосах 5 ГГц U-NII. Использование 40МГц каналов в полосах частот 5 ГГц имеет смысл, потому что существует много 20МГц каналов, которые могут быть объединены вместе в различные пары, как показано на Рисунке 10.19.

**Р И С У Н О К 10.19** Объединение каналов—5 ГГц полосы U-NII



Разворачивание 40МГц каналов в 2,4ГГц, к сожалению, не масштабируется на несколько моделей переиспользования каналов [channel reuse pattern]. Как вы узнали в главах ранее, хотя в 2,4 ГГц и доступно 14 каналов, только три неперекрывающихся 20МГц канала доступно в ISM полосе 2,4 ГГц. Когда меньшие каналы объединяются вместе для образования 40МГц каналов в полосе 2,4ГГц ISM, любые два 40МГц канала будут перекрываться, как показано на Рисунке 10.20. Другими словами, только один 40МГц может быть использован в 2,4 ГГц, и возможность использования модели переиспользования канала, фактически, невозможна.

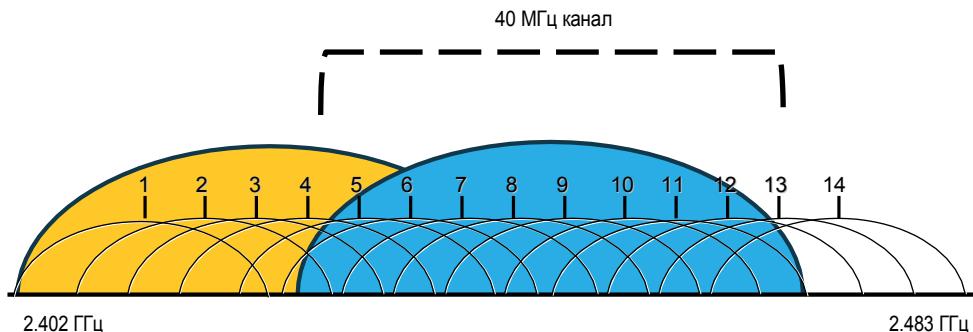
## Сорокамегагерцевая нетолерантность

Как вы только что узнали, только один неперекрывающийся 40 МГц канал может быть развернут в полосе 2,4 ГГц; следовательно, модель переиспользования канала, использующая 40 МГц каналы в 2,4 ГГц является невозможной.

Однако, все еще возможно включить объединение каналов в полосе 2,4 ГГц. 2,4 ГГц точка доступа 802.11n, передающая в 40МГц канале будет интерферировать с другими близлежащими ТД, которые были установлены с использованием стандартной 20МГц модели переиспользования каналов 1, 6 и 11.

По умолчанию, клиентам 802.11n и ТД следует использовать 20 МГц каналы при передаче в полосе 2,4 ГГц. Они также могут сообщать, что они *Нетолерантны к Сороке Мегагерцам [Forty MHz Intolerant]*, используя различные кадры управления 802.11n. Любая ТД 802.11n, использующая 40 МГц канал, принудительно переключается обратно на использование только 20 МГц каналов, если она получит кадры от соседних станций 802.11n 2,4 ГГц, о том, что они нетолерантны.

**РИСУНОК 10.20** Объединение каналов—полоса 2,4 ГГц ISM



Фактически, работа Сорокамегагерцовой Нетолерантности является защищой от вашего ближайшего соседа, который мог развернуть 40 МГц канал, и интерферировать с вашим 20МГц каналами в 2,4 ГГц. Точки доступа БЛВС предприятия должны иметь каналы в 20 МГц в качестве настройки по умолчанию в 2,4 ГГц. Стоить отметить, что работа Сорокамегагерцовой Нетолерантности имеет значение только для 2,4 ГГц, и не разрешена в 5 ГГц.

## Каналы 80 МГц и 160 МГц

802.11ac ввел две дополнительные ширины канала: 80 МГц и 160 МГц. Так же как 40 МГц канал создается путем объединения двух 20 МГц Каналов, 80 МГц канал объединяет четыре 20 МГц канала. Как показано на Рисунке 10.21, 80 МГц канал состоит из 256 поднесущих, 234 из которых используются для передачи данных, 8 используются как контрольные несущие [pilot carriers], а оставшиеся 14 не используются и функционируют как защитные полосы.

Вторая ширина канала, которая была представлена в 802.11ac – это 160 МГц канал. Как вы можете сделать вывод, 160 МГц канал сделан из двух 80 МГц каналов; однако, два 80 МГц канала не обязаны быть смежными. Если каналы смежные, то они называются как 160 МГц канал. Если они не смежные, то они называются как канал 80+80 МГц. Поскольку эти каналы могут быть соседними или отдельными, они рассматриваются как два отдельных 80 МГц канала, и вы не получаете никаких неиспользуемых поднесущих между каналами. Следовательно, канал 160 МГц просто два 80 МГц канала, и состоит из 512 поднесущих с 468, используемых для передачи данных, 16, используемых в качестве контрольных сигналов [pilot carriers], и оставшиеся 28 не используются и работают как защитные полосы.

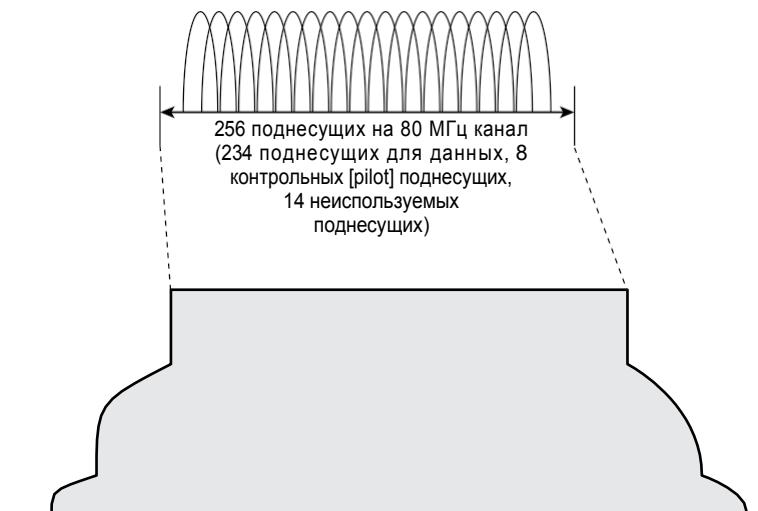
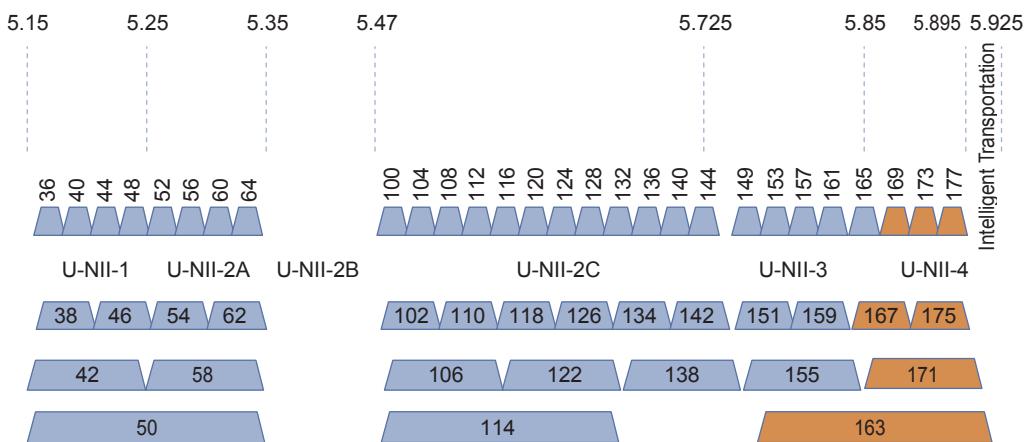
**РИСУНОК 10.21** 80 МГц VHT (802.11ac) канал

Рисунок 10.22 показывает все вариации комбинаций 20 МГц, 40 МГц, 80МГц и смежные 160 МГц каналы в 5 ГГц U-NII полосах. Пожалуйста, обратите внимание, что этот рисунок также показывает предлагаемые каналы U-NII-4, которые еще не доступны для Wi-Fi связи. И хотя каналы 80МГц и 160 МГц доступны в радиомодулях 802.11ac, они не должны использоваться на предприятиях. В Главе 13 “Концепции Проектирования БЛВС” вы узнаете, что дизайн с переиспользованием 20МГц канала все еще является предпочтительным методом. Дизайн с переиспользованием 40МГц каналов может также работать на предприятиях с тщательным планированием. Внедрение каналов 80 МГц и 160 МГц не масштабируются в БЛВС предприятий. В будущем, из-за доступности всего частотного пространства в 6ГГц, ожидается, что использование 40, 80, и даже 160 МГц каналов станут намного более предпочтительными.

**РИСУНОК 10.22** 20, 40, 80, и 160 МГц каналы

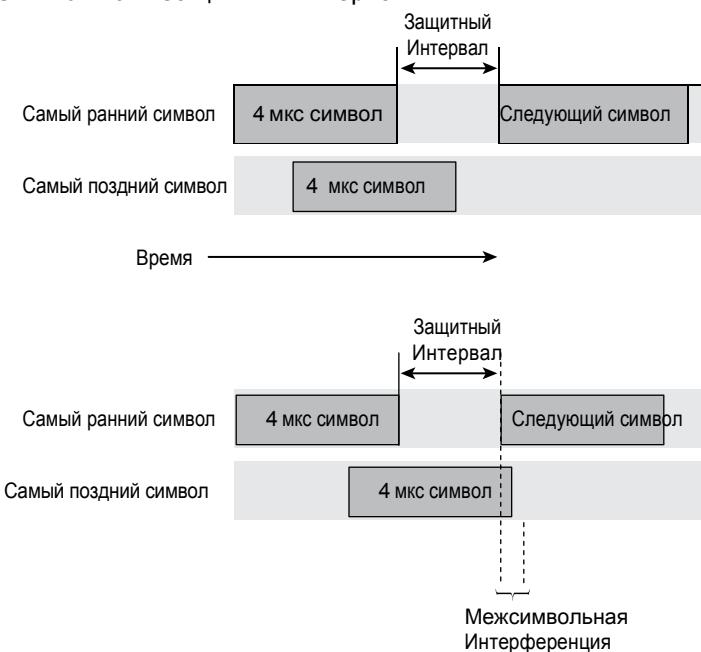
# Защитный Интервал

Для цифровых сигналов, данные модулируются в несущий сигнал в биты или набор битов, называемых *символами [symbols]*. Когда радиомодули передают в 802.11a/g при скорости передачи данных 54 Мбит/с, каждый OFDM символ содержит 288 битов; 216 из этих битов являются данными, а 72 бита являются битами исправления ошибок [еггог-correction bits]. Все биты данных OFDM символа передаются по 48 поднесущим для данных 20МГц не-НТ (non-HT) канала.

Радиомодули 802.11a/g используют 800 наносекундный защитный интервал [*guard interval (GI)*] между OFDM символами. Защитный интервал - это период времени между символами, который вмещает позднее прибытие символов по длинному пути. В среде с многолучевым распространением, символы идут разными путями, поэтому некоторые символы приходят поздно. "Новый" символ может прибыть на приемник до того, как "поздний" символ будет полностью принят. Это называется *межсимвольной интерференцией [intersymbol interference (ISI)]*, и может привести к повреждению данных.

В ранних главах, мы обсуждали ISI и разброс задержки [*delay spread*]. *Разброс задержки [delay spread]* это разница по времени между несколькими путями одного и того же сигнала. Нормальный разброс задержки составляет от 50 наносекунд до 100 наносекунд, а максимальный разброс задержки около 200 наносекунд. Защитный интервал должен быть от двух до четырех раз длиннее разброса задержки. Рассматривайте защитный интервал как буфер для разброса задержки. Обычный защитный интервал - 800 наносекундный буфер между символыми передачами; однако, в большинстве сред внутри помещений, 400 наносекундный буфер обеспечивает достаточное разнесение между передачами. Как показано на Рисунке 10.23, защитный интервал компенсирует разброс задержки и помогает предотвратить межсимвольную интерференцию. Если защитный интервал слишком мал, то межсимвольная интерференция все еще может случаться.

**РИСУНОК 10.23** Защитный интервал



В противоположность популярному мнению, защитный интервал не является пустым эфирным временем. Циклический префикс [*cyclic prefix*] создается таким образом, что каждому символу OFDM предшествует копия конечной части того же самого символа. Как показано на Рисунке 10.24, этот циклический префикс сдвинет негативное влияние многолучевого распространения, которое происходит в течении выделенного периода защитного интервала.

**Р И С У Н О К 1 0 . 2 4** Защитный интервал – циклический префикс

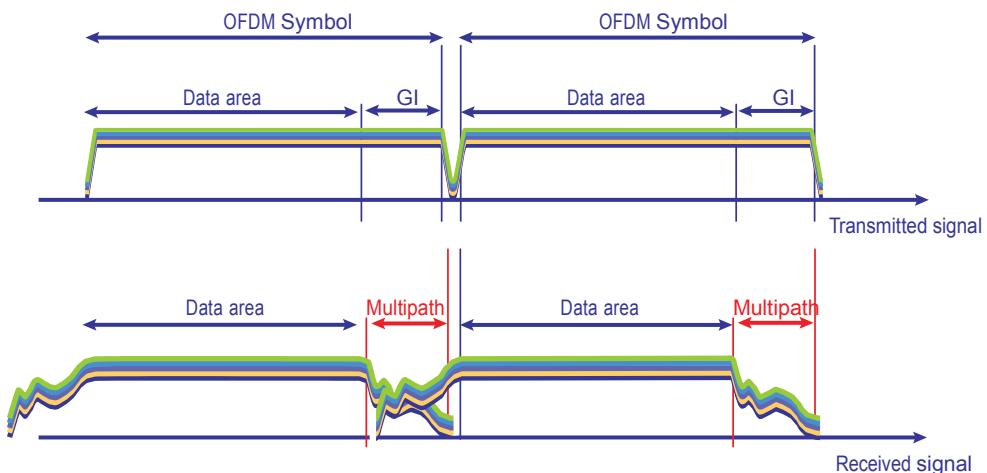


График любезно предоставлен [www.wirelesstrainingsolutions.com](http://www.wirelesstrainingsolutions.com)

Технология 802.11n/ac (HT/VHT) представила возможность установки 400 наносекундного защитного интервала, иногда называемого *короткий защитный интервал* [*short guard interval*]. Радиомодули 802.11n/ac также используют 800 наносекундный защитный интервал; однако, более короткий 400 наносекундный защитный интервал является опциональным. Короткий защитный интервал приводит к короткому символьному времени, эффект от которого - увеличение скорости передачи данных примерно на 10 процентов. Если, дополнительно, использовать более короткий 400 наносекундный защитный интервал в радиомодулях 802.11n/ac, то пропускная способность увеличиваться; однако, и вероятность возникновения межсимвольной интерференции увеличится тоже. Если действительно произойдет межсимвольная интерференция из-за короткого защитного интервала [GI], это приведет к повреждению данных. Если происходит повреждение данных, то увеличивается повторные передачи на 2м уровне, и пропускная способность пострадает. Если пропускная способность упадет из-за настройки короткого GI, то нужно использовать 800 наносекунд в настройках защитного интервала. В большинстве сред внутри помещений короткий защитный интервал в 400 наносекунд является предпочтительным. Длинный защитный интервал может быть необходим внутри помещений в среде с высоким многолучевым распространением. Длинный защитный интервал обычно используется снаружи, вне помещений.

# Модуляция 256-QAM

В Главе 1 "Обзор Беспроводных Стандартов, Организаций и Основ", мы объяснили, как волны манипулируются, или модулируются, для того, чтобы переносить данные. Глава описывала как можно изменять амплитуду, частоту или фазу, чтобы представить один бит данных или даже несколько битов данных. С годами, более новые и быстрые методы модуляции были включены в технологии Физического уровня (PHY) 802.11. С введением каждого нового и быстрого физического уровня (PHY) также вводился и более новый способ модуляции, способный закодировать больше битов, таким образом увеличивая фактическую скорость и производительность сети. Важно помнить, что даже при введении новых способов передачи и модуляции, старые и медленные методы продолжают поддерживаться и использоваться.

По мере того как клиент перемещается от точки доступа и уменьшения силы сигнала, динамическое переключение скорости заставляет клиента переключаться на более медленную скорость передачи данных для поддержки соединения. Даже несмотря на то, что мы стремимся выделить самые последние и величайшие технологии, которые вводятся с самыми последними стандартами и поправками, старые и медленные технологии все еще являются ключевыми и необходимыми компонентами любой инфраструктуры.

Этот раздел описывает 256-QAM, которая была введена с поправкой 802.11ac. (QAM – это акроним от quadrature amplitude modulation [квадратурной амплитудной модуляции] и произносится по-русски “кам”, по-английски “kwam”, и рифмуется с “Tom.”) Далее идет список методов модуляции, которые используются в сетях 802.11:

**DBPSK**—Differential binary phase-shift keying (Дифференциальная двоичная фазовая модуляция)

**DQPSK**—Differential quadrature phase-shift keying (Дифференциальная квадратурная фазовая модуляция)

**BPSK**—Binary phase-shift keying (Двоичная фазовая модуляция)

**QPSK**—Quadrature phase-shift keying (Квадратурная фазовая модуляция)

**16-QAM**—16 quadrature amplitude modulation (Шестнадцатеричная квадратурная амплитудная модуляция)

**64-QAM**—64 quadrature amplitude modulation (Шестьдесятчетыричная квадратурная амплитудная модуляция)

**256-QAM**—256 quadrature amplitude modulation (Дввестипятидесятишестиричная квадратурная амплитудная модуляция)

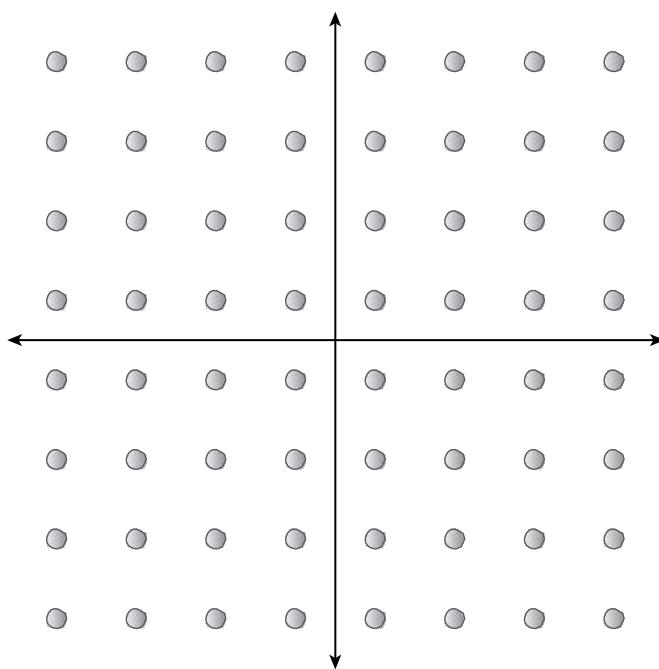
**1024-QAM**—1024 quadrature amplitude modulation (Тысячадвадцатичетыричная квадратурная амплитудная модуляция)

1024-QAM – это последний способ модуляции, введенный в 802.11ax, и будет объяснен в Главе 19. Его предшественник, 256-QAM, был эволюционным улучшением, которое было представлено в 802.11ac. Поправка 802.11a представила модуляцию 64-QAM.

64-QAM идентифицирует 64 уникальных значения. 64-QAM фактически производит

фазовый сдвиг (смену фазы), который может означать восемь разных уровней, а также выполняет амплитудный сдвиг (изменение амплитуды), который также определяет восемь разных уровней. Комбинируем их вместе, и, система получает возможность идентифицировать 64 уникальных значений. Обладание 64 различными значениями дает возможность каждой величине представить 6 битов ( $2^6 = 64$ ). QAM часто представляется символами, изображенными на диаграммах созвездий [constellation chart], как показано на Рисунке 10.25. Каждая точка представляет уникальный символ – разные группы из 6 битов.

РИСУНОК 10.25 Диаграмма созвездия [constellation chart] 64-QAM

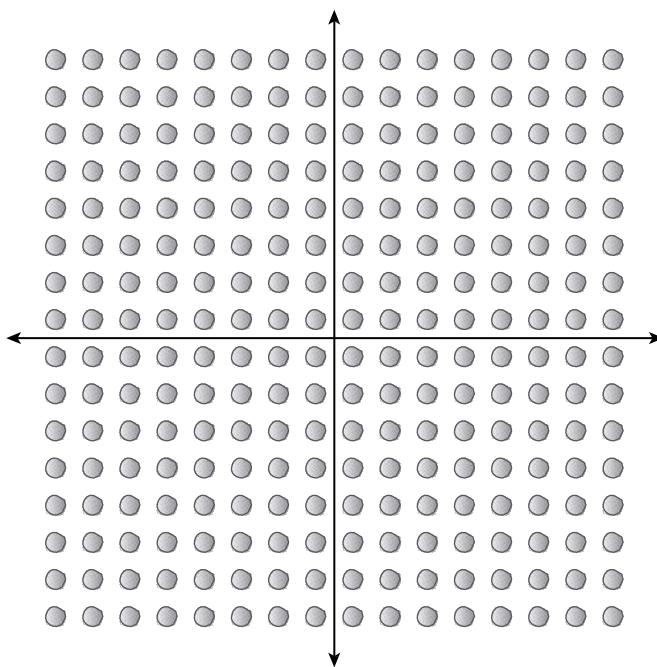


256-QAM определяет 256 уникальных величин, используя 16 различных уровней фазового сдвига и 16 различных уровней амплитудного сдвига. Так как существует 256 отдельных значений, каждое значение способно представить 8 бит ( $2^8 = 256$ ).

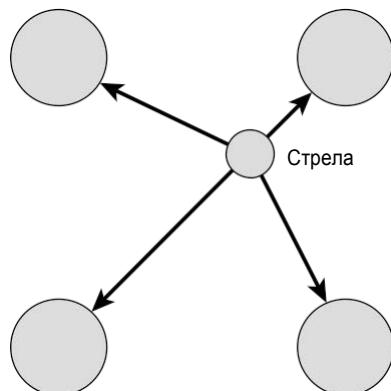
Рисунок 10.26 показывает диаграмму созвездия для 256-QAM.

Теперь, когда мы предоставили базовое объяснение 64-QAM и 256-QAM, нам нужно копнуть немного глубже так, чтобы вы поняли, что происходит и как они отличаются. Когда радиомодуль 64-QAM передает данные, он модифицирует амплитуду и фазу волны, а затем передает ее. Приемный радиомодуль должен затем принять сигнал и определить модификации амплитуды и фазы, которые были сделаны, чтобы определить какой из 64 символов был передан. Это не всегда просто, так как шум и интерференция могут сделать сложным идентификацию значения переданного сигнала.

В качестве аналогии, представьте лучника, стреляющего стрелами в мишень. Допустим, что мишень – это 2х метровая квадратная доска с равномерно расположенными одно-дюймовыми точками по восемь штук в ряду и в столбце. Мишень стоит на крыше здания, которое мы будем называть целевой крышей. В десяти метрах от целевой крыши есть еще одна крыша, где стоит Олимпийский лучник. Мы будем называть эту крышу – стрелковой крышей. В идеальных условиях, наш Олимпийский стрелок никогда не промахивается. Однако, пространство между этими двумя зданиями непредсказуемо ветрено, не только из стороны в сторону, но также и с восходящими и нисходящими потоками. На стрелковой крыше мы просим лучника запустить стрелу в определенную точку на мишени. Так как ветры так непредсказуемы, то лучник не делает никаких поправок и коррекций, а только целился в выбранную точку и надеется, что ветры не столкнут стрелу очень далеко от цели.

**РИСУНОК 10.26** Диаграмма созвездия [constellation chart] 256-QAM

Когда стрела попадает в мишень, человек на целевой крыше рассматривает местоположение стрелы, и, используя рулетку, измеряет расстояние от стрелы до ближайшей точки, и пытается определить в какую точку стрелял лучник. Как пример, Рисунок 10.27 показывает четыре точки и местоположение, куда попала стрела. На этой картинке, человек вероятно определит точку в правом верхнем углу, как точку, в которую целился лучник. При таком коротком расстоянии, до тех пор, пока ветер не будет невероятно сильным, лучник сможет запускать стрелы точно в или рядом с выбранной точкой, а человек около мишени сможет правильно определять в какую точку целился лучник.

**РИСУНОК 10.27** Пример мишени

Если мы постепенно сдвинем лучника дальше от мишени, то ветер будет больше мешать полету стрелы, возможно даже заставляя ее смещаться дальше от точки, в которую целился лучник. Чем дальше от мишени, тем менее удачным будет лучник. 64-QAM ведет себя похоже. Передающий радиомодуль модулирует сигнал и передает его. Амплитудная и фазовая подстройка является точной, и радиомодулем генерируется идеальный модулированный сигнал. Шум, интерференция, и затухание (attenuation) сигнала изменяют сигнал так, что, когда он принят, он уже модифицирован. Приемник проецирует сигнал на диаграмму созвездия [constellation diagram] и вычисляет вектор ошибки, чтобы определить точку созвездия, которая соответствует переданным данным. Величина вектора ошибки [*Error vector magnitude (EVM)*] является мерой, используемой для измерения производительности радиоприемника или радиопередатчика относительно точности модуляции. В модуляции QAM, EVM - это мера того, как далеко находится полученный сигнал от точки созвездия.

Итак, теперь, когда у вас есть общая идея того как ведет себя 64-QAM, как это относится к 256-QAM? Это довольно просто. В нашей аналогии с лучником, вместо 64 точек на мишени, мы используем мишень того же размера, но размещаем на ней 256 точек. Это означает, что теперь меньше пространства для ошибки, таким образом расстояние лучника от мишени и влияние ветра на стрелу являются на много более критичными. Точно так же, 256-QAM является более чувствительной к шуму и интерференции. Из-за этого, производительность приемника 802.11ac требует дополнительно примерно на 5 dB больше, по сравнению с 64-QAM. Чтобы радиомодуль 802.11ac использовал модуляцию 256-QAM, требуется соотношение сигнал-шум (SNR) 29dB или больше.

256-QAM используется для самых высоких кодирующих наборов модуляции. Чтобы достичь этих высоких скоростей передачи данных, нужны более высокие соотношения сигнал-шум. Это также означает, что клиентам нужно быть ближе к ТД, чтобы достичь эти скорости передачи данных. Поскольку сигнал с 256-QAM может передать 8 бит на поднесущую, по сравнению с 6 битами, которые передавались с 64-QAM, увеличение скорости на 33 процента достигается только за счет внедрения этой функции.

Как упоминалось ранее, 802.11ac поддерживается только в полосах 5ГГц. Самая скоростная модуляция, официально поддерживаемая поправкой 802.11n, - это 64-QAM. В двухдиапазонных радиомодулях 802.11ac, хотя 256-QAM и не является частью стандарта 802.11n, эта технология уже интегрирована в микросхемы (чипы или чипсеты) радиомодулей 802.11ac.



Хотя 802.11ac только для 5 ГГц радиомодулей, некоторые производители БЛВС предлагают поддержку 256-QAM для радиомодулей точек доступа 802.11n в 2,4ГГц. Турбо-QAM – это маркетинговый термин компании Broadcom (Broadcom) для нестандартной поддержки 256-QAM в радиомодулях в 2,4ГГц. Чтобы этот функционал работал, клиенты также должны поддерживать 256-QAM в своих радиомодулях 2,4ГГц. Кроме того, достижение необходимого SNR для 256-QAM обычно является непростой амбициозной задачей из-за очень высокого уровня шума, который обычно присутствует в полосе 2,4 ГГц.

## 802.11n/ac PPDU

В главах ранее, вы узнали, что блок сервисных данных MAC [MAC service data unit (MSDU)] является полезной нагрузкой уровней 3-7 кадра данных 802.11. Вы также узнали, что блок протокола данных MAC [MAC protocol data unit (MPDU)] является техническим названием целого кадра 802.11. MPDU состоит из заголовка, тела и окончания 2ого уровня.

Когда MPDU (кадр 802.11) посыпается вниз с уровня 2 на Физический уровень, преамбула [preamble] и заголовок физического уровня (PHY) добавляются к MPDU. Это создает, что называется *блоком данных протокола Процедуры Сходимости Физического Уровня [Physical Layer Convergence Procedure protocol data unit (PPDU)]*.

Подробности преамбулы и заголовка PHY находятся далеко за пределами экзамена CWNA. Основное назначение преамбулы – использовать биты для синхронизации передачи на Физическом уровне между двумя радиомодулями 802.11. Основное назначение заголовка PHY – использовать поле сигнала для обозначения длительности передачи кадра 802.11 (MPDU) и уведомления приемника о MCS (скорости передачи данных), которое будет использоваться для передачи MPDU. Стандарт 802.11-2020 определяет использование нескольких структур и преамбул PPDU. И 802.11n и 802.11ac представили новые заголовки PHY.

### Non-HT

Первый формат PPDU называется *не-HT [non-HT]* и часто называется, как устаревший формат, потому что он изначально определял передачи OFDM. Как показано на Рисунке 10.28, не-HT [non-HT] PPDU содержит преамбулу, которая использует устаревшие короткие и длинные тренировочные символы для синхронизации.

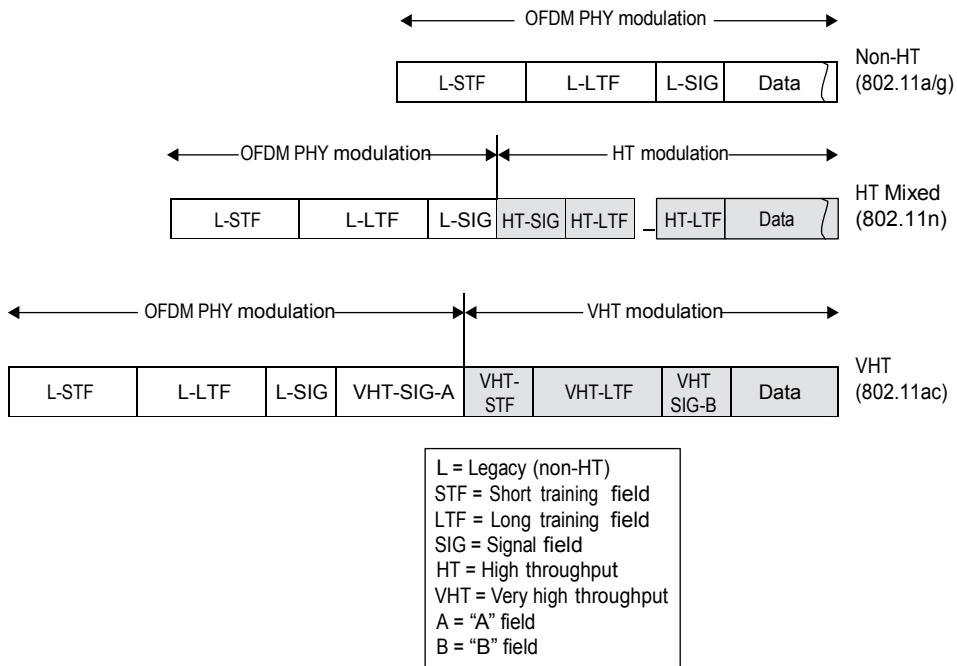
OFDM символ состоит из 12 битов. Заголовок содержит поле сигнала, которое показывает время, необходимое для передачи полезной нагрузки не-HT PPDU, который, конечно, является MPDU (кадром 802.11). Поддержка устаревшего не-HT формата является обязательной для радиомодулей 802.11n, и передачи могут происходить только в 20 МГц каналах. Не-HT [non-HT] формат фактически является тем же самым форматом, используемым устаревшими радиомодулями 802.11a и 802.11g.

### HT Mixed

Второй формат PPDU – это смешанный HT формат [*HT Mixed format*]. Как показано на Рисунке 10.28, начало преамбулы содержит тренировочные символы не-HT [non-HT] и устаревшее поле сигнала, которые могут быть декодированы устаревшими радиомодулями 802.11a и 802.11g. Остальное преамбулы и заголовка Смешанного HT [HT Mixed] не может быть декодировано устаревшими устройствами 802.11a/g. Информация HT включает тренировочные символы HT-SIG и HT.

HT Сигнал [HT Signal (HT-SIG)] содержит информацию о MCS, длине кадра, 20МГц или 40 МГц размер канала, агрегации кадров, защитном интервале, и STBC. Поле Короткой Тренировочной последовательности HT [HT Short Training Field (HT-STF)] и Поле Длинной Тренировочной последовательности [HT Long Training Field (HT-LTF)] используются для синхронизации между радиомодулями MIMO.

**РИСУНОК 10.28** Форматы PPDU



Не-802.11n приемники не смогут прочитать кадр, но поле длины в устаревшем разделе заголовка позволит им знать, как долго среда будет занята, и, следовательно, они будут молчать без необходимости выполнять обнаружение энергии [energy detect] в каждом цикле. Смешанный формат НТ [HT Mixed format] поддерживает и НТ и старые 802.11a/g OFDM радиомодули. Смешанный формат [HT Mixed] также считается обязательным, и передачи могут осуществляться и в 20МГц и в 40 МГц каналах. Когда используется 40 МГц канал, весь широковещательный(broadcast) трафик должен быть передан по устаревшим 20 МГц каналам, для того чтобы поддержать совместимость с 802.11a/g не-НТ [non-HT] клиентами. Также, любые передачи к и от не-НТ [non-HT] клиентов должны будут использовать устаревший 20МГц канал.

## VHT

Финальный формат PPDU - это формат VHT для радиомодулей 802.11ac. Как показано на Рисунке 10.28, преамбула совместима как с устаревшими радиомодулями 802.11a/g, так и с радиомодулями 802.11n. Не-VHT [non-VHT] часть заголовка PHY могут понять устаревшие устройства 802.11a/n, в то время как VHT часть заголовка PHY могут понять только радиомодули 802.11ac. VHT часть заголовка PHY может быть использована для обозначения могут ли или нет происходить передачи SU-MIMO или MU-MIMO.

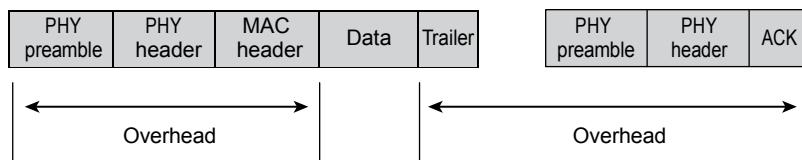
## 802.11n/ac MAC

Итак, мы обсудили все расширения Физического уровня, которые используют радиомодули ММО, чтобы получить большую ширину полосы и пропускную способность. Стандарт 802.11-2020 также расширяет MAC подуровень Канального [Data-Link] уровня, чтобы увеличить пропускную способность и улучшить управление питанием. Накладные расходы [overhead] борьбы за среду адресуются использованию двух методов агрегации кадров. Улучшения также адресуются блоковым подтверждениям для ограничения фиксированных служебных данных MAC [MAC overhead]. Определено три метода управления питанием для радиомодулей ММО.

### A-MSDU

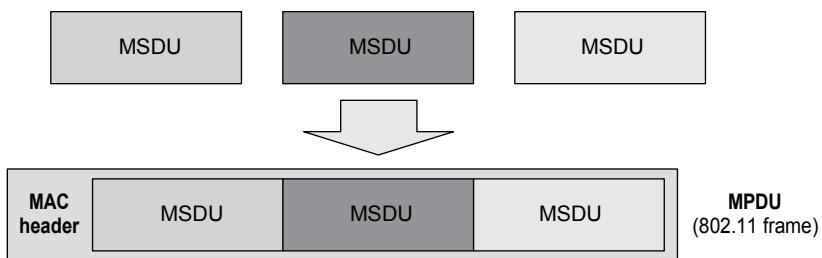
Как вы можете видеть на Рисунке 10.29, каждый раз, когда передается одноточечный [unicast] кадр 802.11, существует определенное количество фиксированной служебной информации (накладных расходов или overhead) из-за заголовка PHY, заголовка MAC, окончания MAC, межкадрового пространства, и кадра подтверждения. Накладные расходы (оверхед) при борьбе за среду также существуют из-за времени, требуемого, когда каждый кадр должен бороться за среду.

**Р И С У Н О К 10 . 2 9** Служебная информация[overhead] одноточечного[unicast] кадра 802.11



Поправка 802.11n представила два метода агрегации кадров, чтобы помочь уменьшить служебную информацию [overhead]. *Агрегация кадров* [Frame aggregation] – это метод объединения нескольких кадров в передачу единого кадра. Фиксированные накладные расходы MAC уровня уменьшены, и накладные расходы [overhead] вызванные случаем обратным таймером во время борьбы за среду также минимизированы.

Первый метод агрегации кадров называется *агрегированный блок сервисных данных MAC* [aggregate MAC service data unit (*A-MSDU*)]. Как вы узнали в ранних главах, MSDU – это полезная нагрузка кадра данных уровней 3-7. Как показывает Рисунок 10.30, несколько MSDU смогут быть агрегированы в один кадр передачи.

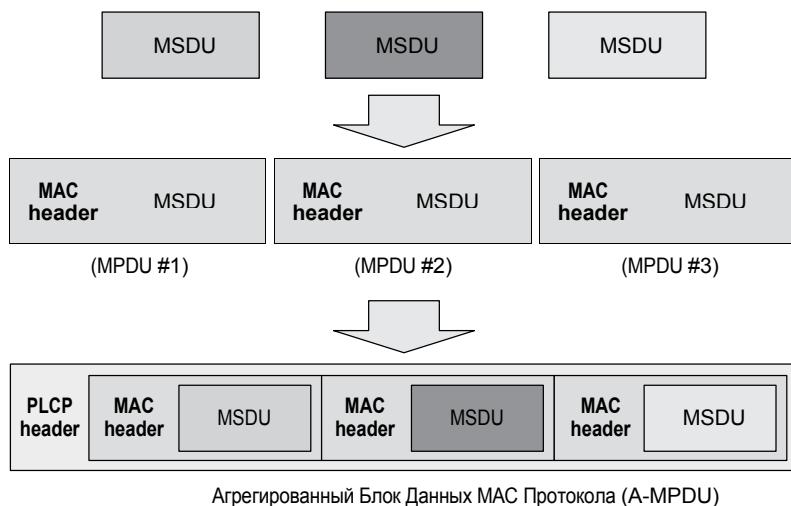
**Р И С У Н О К 1 0 . 3 0** A-MSDU

Точка доступа MIMO, использующая агрегацию A-MSDU, будет получать несколько кадров 802.3, убирать заголовки 802.3 и окончания, а затем обворачивать несколько полезных нагрузок MSDU в один кадр 802.11 для передачи. Агрегированные MSDU будут иметь один беспроводной приемник, когда все вместе упакованы в один кадр. Все MSDU внутри A-MSDU зашифрованы, как одна зашифрованная полезная нагрузка. Стоит, однако, отметить, что все MSDU по отдельности должны быть одной и той же категории доступа QoS. Например, Голосовой MSDU не может быть смешан с MSDU Обычного трафика (Best-Effort) или MSDU Видео внутри одного и того же агрегированного кадра. Во многих первоначальных микросхемах (чипах) 802.11n встроена поддержка A-MSDU.

## A-MPDU

Второй метод агрегации кадров называется *агрегация блока данных MAC протокола* [*aggregate MAC protocol data unit (A-MPDU)*]. Как вы узнали в ранних главах, MPDU это весь кадр 802.11, включая MAC заголовок, тело и окончание. Как показано на Рисунке 10.31, несколько MPDU может быть агрегировано в одну передачу PPDU. Заметьте, что на Рисунке 10.31 A-MPDU включает в себя несколько MPDU и прикрепленный в начале заголовок PHY.

**Р И С У Н О К 1 0 . 3 1** A-MPDU



Отдельные MPDU внутри A-MPDU должны все иметь один и тот же адрес получателя. В отличие от A-MSDU, полезная нагрузка каждого MPDU шифруется и дешифруется отдельно. Почти так же как агрегация MSDU, индивидуальные MPDU должны все быть одной и той же категории доступа QoS 802.11e. Голосовые MPDU не могут быть смешаны с Best Effort или Видео MPDU внутри одного и того же агрегированного кадра. Обратите внимание, что агрегация MPDU имеет больше служебной информации, чем агрегация MSDU, потому что каждый MPDU имеет свой индивидуальный MAC заголовок и окончание.

Однако, A-MPDU использует Блоковые ACK для подтверждения доставки, в то время как A-MSDU использует ACK для подтверждения доставки. Кадр A-MPDU уменьшает по кадровую служебную информацию (overhead) и требует только одно Блоковое ACK. Ошибки CRC могут быть обнаружены в индивидуальных кадрах MPDU, а, следовательно, весь A-MPDU не нужно отправлять заново, только отдельный MPDU, который поврежден. Следовательно, A-MPDU менее восприимчив к шуму, чем A-MSDU. По этой причине, большинство производителей БЛВС выбирают использование A-MPDU во втором поколении чипов(чипсетов) 802.11n.

Поправка 802.11ac определяет только использование A-MPDU агрегацию. Все кадры 802.11ac передаются, используя формат агрегированного блока данных MAC протокола (A-MPDU), даже если только передает один кадр. Хотя A-MPDU требуется для передачи 802.11ac, стоит отметить, что A-MSDU и A-MPDU могут быть использованы вместе. Полезной нагрузкой передачи A-MPDU может быть несколько A-MSDU.

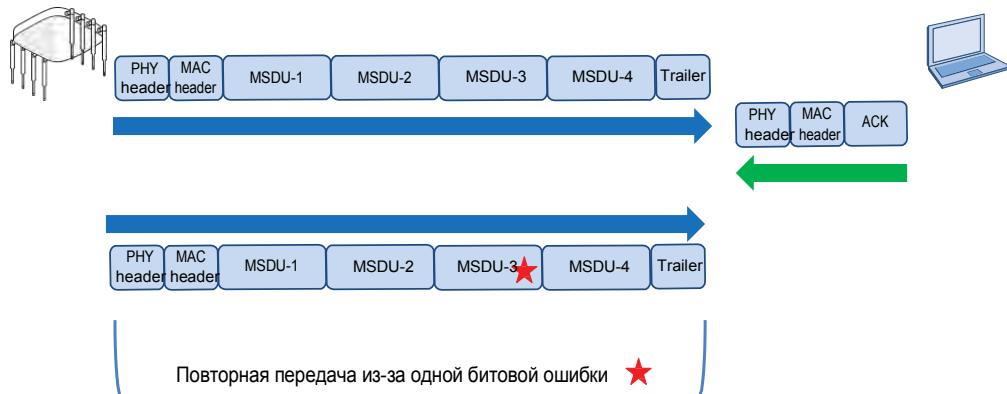
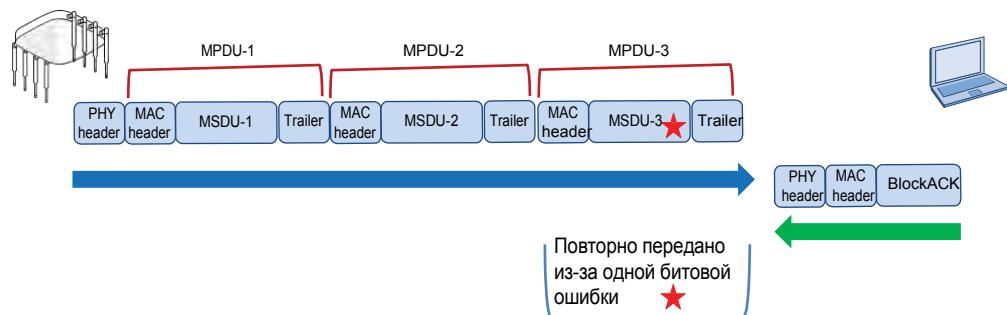
## Блоковое Подтверждение

Как вы узнали в ранних главах, за всеми одноточечными (unicast) кадрами 802.11 должны следовать кадры ACK в целях подтверждения доставки. Многовещательные (multicast) и Широковещательные (Broadcast) кадры не подтверждаются. Кадр A-MSDU содержит несколько MSDU, обернутых в один кадр с одним MAC заголовком и одним получателем. Следовательно, требуется одно обычное подтверждение, при использовании агрегации A-MSDU. Однако, кадр A-MPDU содержит несколько MPDU, каждый со своим уникальным MAC заголовком. Каждый индивидуальный MPDU должен быть подтвержден; это выполняется путем использования кадра Блокового ACK (Блокового Подтверждения). Блоковые ACK (подтверждения), были впервые представлены в поправке 802.11e, как способ подтверждения нескольких индивидуальных кадров 802.11 во время *взрыв из кадров* [*frame burst*]. Блоковые подтверждения также нужны чтобы охватить несколько MPDU, которые агрегированы внутри одной передачи A-MPDU.

Как показано на Рисунке 10.32, когда используется агрегация A-MSDU, используется стандартный кадр 802.11 ACK, чтобы подтвердить доставку передачи A-MSDU. Звезда на обоих Рисунках 10.32 и 10.33 обозначает один поврежденный бит. Если любая часть кадра A-MSDU повреждена, получатель не ответит кадром ACK, а весь кадр A-MSDU должен быть отправлен повторно. Как изображено на Рисунке 10.33, в агрегации A-MPDU, если один из MPDU поврежден, то Блоковое ACK проинформирует передатчик о том, какой MPDU поврежден. Только поврежденный MPDU должен быть отправлен повторно, а не весь A-MPDU. Метод A-MPDU более эффективен, чем A-MSDU, из-за использования Блоковых ACK и меньших повторных передач служебной информации. Это главная причина, по которой A-MPDU требуется для радиомодулей 802.11ac.

## Управление Питанием

Так как в стандарт 802.11 вносятся поправки, функционал управления питанием продолжает улучшаться. Поправка 802.11e QoS ввела *незапланированное предоставление автоматического сбережения энергии* [*unscheduled automatic power save delivery (U-APSD)*], которое является механизмом, используемым Сбережением Энергии WMM [WMM Power Save (WMM-PS)]. Поправка 802.11n представила два механизма управления питанием, которые используются радиомодулями 802.11n (HT). Механизмы управления питанием 802.11n считаются дополнительными к WMM-PS, когда используются радиомодули MIMO.

**РИСУНОК 10.32** A-MSDU, ACKs, и повторные передачи**РИСУНОК 10.33** A-MPDU, Block ACKs, и повторные передачи

Радиомодули 802.11n/ac все еще поддерживают базовый режим экономии энергии, который основан на изначальных механизмах управления питанием 802.11. Точки доступа буферизируют кадры для станций в базовом режиме экономии энергии. Станции просыпаются, когда происходит широкое вещание (broadcast) маяков с сообщениями-индикаторами о доставке трафика [delivery traffic indication message (DTIM) beacons] и станции загружают свои забуферизованные кадры.

Первый метод управления питанием, представленный в 802.11n, называется *сбережение энергии пространственного мультиплексирования* [*spatial multiplexing power save (SM power save)*]. Цель экономии энергии пространственного мультиплексирования [SM power save] в разрешении устройствам MIMO 802.11ac выключать все, кроме одного, свои радиомодули.

Например, устройство 4×4 MIMO с четырьмя радиотехническими цепями выключают три из четырех радиомодулей, таким образом сберегая энергию. Сбережение энергии пространственного мультиплексирования [SM power save] определяет два способа работы: статический и динамический.

Когда используется статическое сбережение энергии пространственного мультиплексирования [SM power save], клиентская станция MIMO выключает по питанию все клиентские радиомодули, кроме одного радиомодуля. Фактически, клиентская станция MIMO теперь эквивалентна радиомодулю SISO, который может посылать и принимать только один пространственный поток. Клиент использует кадр действия [SM power save], чтобы проинформировать точку доступа, что MIMO клиент использует только один радиомодуль и способен принимать только один пространственный поток от ТД.

Кадр действия сбережения энергии пространственного мультиплексирования [SM power save action frame] также используется, чтобы сказать точке доступа, что клиентская станция включила все свои радиомодули, и теперь способна передавать и принимать несколько пространственных потоков снова.

Когда используется динамическое сбережение энергии пространственного мультиплексирования [SM power save], MIMO клиент может также выключить все, кроме одного, радиомодули, но может включить радиомодули снова намного быстрее. Клиентская станция деактивирует все, кроме одного, радиомодули после обмена кадрами. Точка доступа может дать команду клиенту, чтобы разбудить спящие радиомодули, путем отправки кадра запроса-на-отправку [request-to-send (RTS)]. Клиентская станция получает кадр RTS, включает спящие радиомодули, и посыпается кадр чисто-для-отправки [clear- to-send (CTS)] обратно точке доступа. Теперь клиент снова может передавать и принимать несколько пространственных потоков. Клиент использует кадр действия пространственного мультиплексирования [SM power save] чтобы проинформировать ТД о состоянии клиентского динамического сбережения энергии.

Второй метод управления питанием, представленный в 802.11n, - это *много-опросное сбережение энергии [power save multi-poll (PSMP)]*. PSMP - это расширение предоставления автоматического сбережения энергии [automatic power save delivery (APSD)], которое было определено поправкой 802.11e. Незапланированное много-опросное сбережение энергии [Unscheduled PSMP (U-PSMP)] похоже на U-APSD, и использует те же самые механизмы доставки и триггерные механизмы. Плановое много-опросное сбережение энергии [Scheduled PSMP (S-PSMP)] также похоже на S-APSD и является эффективным методом для потоковых данных и других запланированных передач по расписанию. S-PSMP использует кадр, кадр действия PSMP, чтобы запланировать нисходящие [downlink] и восходящие [uplink] передачи. Время нисходящей передачи PSMP [PSMP downlink transmission time (DTT)] - это время, запланированное для ТД для передачи своим присоединенным станциям, а время восходящей передачи PSPM [PSMP uplink transmission time (UTT)] - это время, запланированное для станций, для передачи к ТД.

*Сбережение энергии VHT TXOP [VHT TXOP power save]* это еще один способ управления питанием, который был представлен как часть поправки 802.11ac. Если клиент видит, что *возможность передачи [transmit opportunity (TXOP)]* занята для другого клиента, сбережение энергии VHT TXOP позволяет клиенту выключить свои радиомодули на время передачи. TXOP может происходить на нескольких кадрах, которые могут позволить клиенту вздренуть на больший период времени. ТД должна гарантированно помнить, что клиент недоступен в течении этого времени, и не пытаться отправлять какие либо кадры дремлющему клиенту.

## Схемы Кодирования и Модуляции

Скорости передачи данных 802.11n определены в матрице *схем кодирования и модуляции [modulation and coding scheme (MCS)]*. Не-НТ[non -HT], которые используют OFDM технологию (802.11a/g), используют скорости передачи данных от 6Мбит/с до 54 Мбит/с, базируясь на используемой схемы кодирования и модуляции. НТ радиомодули, однако, определяют скорости передачи данных, базируясь на многочисленных факторах, включая модуляцию, метод кодирования, число пространственных потоков, размер канала, и защитного интервала. Каждая схема кодирования и модуляции [modulation and coding scheme (MCS)] является вариацией этих нескольких факторов. Семьдесят семь схем кодирования и модуляций (MCS) существует для 20МГц НТ каналов и 40 МГц НТ каналов. Восемь схем кодирования и модуляций являются *обязательными [mandatory]* для 20МГц НТ каналов, как показано в Таблице 10.2. Восемь обязательных MCS для 20МГц НТ каналов сравнимы с базовыми(требуемыми) скоростями.

**ТАБЛИЦА 10.2** MCS—20 МГц НТ канал, один пространственный поток

Индекс MCS	Модуляция	Пространственные Потоки	Скорости Передачи Данных	
			800 ns GI	400 ns GI
0	BPSK	1	6.5 Мбит/с	7.2 Мбит/с
1	QPSK	1	13.0 Мбит/с	14.4 Мбит/с
2	QPSK	1	19.5 Мбит/с	21.7 Мбит/с
3	16-QAM	1	26.0 Мбит/с	28.9 Мбит/с
4	16-QAM	1	39.0 Мбит/с	43.3 Мбит/с
5	64-QAM	1	52.0 Мбит/с	57.8 Мбит/с
6	64-QAM	1	58.5 Мбит/с	65.0 Мбит/с
7	64-QAM	1	65.0 Мбит/с	72.2 Мбит/с

Как вы можете видеть в Таблице 10.2, тип модуляции, защитный интервал, и число пространственных потоков - все определяют итоговую скорость передачи данных. Таблица 10.3 описывает схемы кодирования и модуляции для 40МГц канала, использующего четыре пространственных потока.

**ТАБЛИЦА 10.3** MCS—40 МГц НТ канал, четыре пространственных потока

Индекс MCS	Модуляция	Пространственные Потоки	Скорости Передачи Данных	
			800 ns GI	400 ns GI
24	BPSK	4	54.0 Мбит/с	60.0 Мбит/с
25	QPSK	4	108.0 Мбит/с	120.0 Мбит/с
26	QPSK	4	162.0 Мбит/с	180.0 Мбит/с
27	16-QAM	4	216.0 Мбит/с	240.0 Мбит/с
28	16-QAM	4	324.0 Мбит/с	360.0 Мбит/с
29	64-QAM	4	432.0 Мбит/с	480.0 Мбит/с
30	64-QAM	4	486.0 Мбит/с	540.0 Мбит/с
31	64-QAM	4	540.0 Мбит/с	600.0 Мбит/с

802.11n (HT) определяет 77 различных схем кодирования и модуляций [modulation and coding schemes (MCSs)]. HT радиомодули определяют MCSы, базируясь на многочисленных факторах, включая модуляцию, метод кодирования, число пространственных потоков, размер канала и защитного интервала. 802.11n также определяет MCSs, которые допускают неодинаковую модуляцию, которая использует различные модуляции и схемы кодирования в одно и то же время на разных пространственных потоках. 802.11ac (VHT) упростила это путем определения только 10 опций MCS, как показано в Таблице 10.4.

**ТАБЛИЦА 10.4** VHT MCS, модуляция, скорость кодирования, и скорость передачи данных

Значение VHT MCS	Модуляция	Скорость Кодирования(R)	20 МГц Скорость передачи Данных (Мбит/с)
0	BPSK	1/2	7.2
1	QPSK	1/2	14.4
2	QPSK	3/4	21.7
3	16-QAM	1/2	28.9
4	16-QAM	3/4	43.3
5	64-QAM	2/3	57.8
6	64-QAM	3/4	65.0
7	64-QAM	5/6	72.2
8	256-QAM	3/4	86.7
9	256-QAM	5/6	96.3*

\* MCS 9 поддерживается только для 40МГц, 80 МГц и 160 МГц каналов, и не поддерживается для 20 МГц каналов.

Первые восемь схем кодирования и модуляций являются обязательными; однако, большинство производителей поддерживают последние два, которые обеспечивают модуляцию 256-QAM. Столбец Скорость Кодирования [Code Rate (R)] показывает код исправления-ошибок, используемый каждой MCS. Коды исправления ошибок [Error-correcting codes] добавляют резервную информацию, чтобы помочь с исправлением ошибки. Скорость кодирования представляется в виде дроби. Первое число (числитель) представляет количество бит пользовательских данных, относительно к числу битов в канале (делитель) – чем выше кодовая скорость, тем больше данных передается и предоставляется меньше резервирования. Последний столбец представляет максимально достижимую скорость передачи данных для каждой MCS. Скорость передачи данных основывается на 20 МГц канале, одном пространственном потоке, и коротком защитном интервале (400нс).

## Скорости Передачи Данных 802.11ac

Нет какого-то одного улучшения или расширения, которое обеспечивает 802.11ac ее более быстрыми скоростями передачами данных, это комбинация улучшений и расширений. Этот раздел рассмотрит ключевые компоненты, связанные с увеличенной производительностью, и опишет как 802.11ac может похвастаться теоретической скоростью передачи данных вплоть до 6933,3 Мбит/с.

Первое улучшение в отношении увеличенной скорости передачи данных 802.11ac - это 256QAM. Она включена в MCS 8 и MCS 9. Таблица 10.5 показывает максимальную скорость передачи данных для каждой MCS, работающей в одном пространственном потоке и 20МГц канале, и использующем 400нс короткий защитный интервал. По техническим и практическим причинам, некоторые номера MCS не поддерживаются с определенными ширинами каналов и комбинацией пространственных потоков. Существует 10 таких случаев. MCS 6 не поддерживается для 80 МГц канала, при использовании трех или семи пространственных каналов. MCS 9 имеет больше исключений. Она не работает с 20 МГц каналом с использованием одного, двух, четырех, пяти, семи или восьми пространственных потоков. Она не работает с 80 МГц каналом с шестью пространственными потоками, и не работает со 160 МГц каналом с тремя пространственными потоками.

**ТАБЛИЦА 10.5** Факторы скорости передачи данных 802.11ac

MCS	20 МГц Скорость Передачи Данных	Множитель Пространственных Потоков	Множитель Ширины Каналы
0	7.2	× 1 (1 поток)	× 1.0 (20 МГц)
1	14.4	× 2 (2 потока)	× 2.1 (40 МГц)
2	21.7	× 3 (3 потока)	× 4.5 (80 МГц)
3	28.9	× 4 (4 потока)	× 9.0 (160 МГц)
4	43.3	× 5 (5 потоков)	
5	57.8	× 6 (6 потоков)	
6	65.0	× 7 (7 потоков)	
7	72.2	× 8 (8 потоков)	
8	86.7		
9*	96.3		

\* MCS 9 поддерживается только для 40,80 и 160 МГц каналов, и не поддерживается для 20 МГц каналов.

Как показано в Таблице 10.5, даже несмотря на то, что существует только 10 MCS для VHT, существует еще две других переменных, которые определяют скорость передачи данных. Каждый MCS может использовать до восьми пространственных потоков и четырех каналов различной ширины. Каждый пространственный поток способен передавать со скоростью передачи данных, предоставляемой MCS, который используется при передаче. Вычисление увеличения скорости передачи данных это просто дело умножения скорости передачи 20МГц канала на число пространственных потоков, как показано в столбце Множитель Пространственных Потоков в Таблице 10.5.

Последний переменный фактор в увеличении скорости передачи данных - это ширина канала. Ранее в этой главе мы объяснили, что, когда объединяются каналы, мы не только увеличиваем пропускную способность из-за удвоения канала, но также получаем немного больше канального пространства из области между двумя объединенными каналами. Следовательно, увеличение для 40МГц канала - в 2,1 раз, а увеличение для 80МГц канала - в 4,5 раза. Поскольку 160МГц канал состоит из двух 80МГц каналов, соседних или разделенных, то дополнительного увеличения нет. Множитель для 160МГц канала - это просто удвоение результата 80МГц канала, т.е 9 раз.

Таблица 10.6 показывает максимальную скорость передачи данных по каждой ширине канала для каждой MCS при работе по одному пространственному потоку и использовании 400нс короткого защитного интервала.

**ТАБЛИЦА 10.6** Максимальная скорость передачи данных (Мбит/с) – VHT

MCS	20 МГц	40 МГц	80 МГц	160 МГц
0	7.2	15.0	32.5	65.0
1	14.4	30.0	65.0	130.0
2	21.7	45.0	97.5	195.0
3	28.9	60.0	130.0	260.0
4	43.3	90.0	195.0	390.0
5	57.8	120.0	260.0	520.0
6	65.0	135.0	292.5	585.0
7	72.2	150.0	325.0	650.0
8	86.7	180.0	390.0	780.0
9	96.3*	200.0	433.3	866.7

\* MCS 9 поддерживается только для 40,80 и 160 МГц каналов, и не поддерживается для 20 МГц каналов.

Еще не запутались? Хотя 802.11ac определяет только 10 MCS, существует еще более 300 возможных скоростей передачи данных VHT в зависимости от переменных защитного интервала, пространственных потоков, и ширины канала. И как ранее упоминалось, существует 77 MCS для 802.11n, которые определяют скорости передачи данных HT. От вас не ожидают, что вы запомните все возможные комбинации скоростей передачи данных для экзамена CWNA. Однако, хороший справочник для скоростей передачи данных для 802.11n/ac/ax доступен по адресу [www.mcsindex.com](http://www.mcsindex.com).

## Механизмы Защиты HT/VHT

В ранних главах вы узнали о механизмах защиты, используемых в сети ERP (802.11g). Механизмы RTS/CTS и CTS-to-Self используются, чтобы гарантировать, что клиенты 802.11b HR-DSSS не передают, когда происходит передача ERP-OFDM. Радиомодули 802.11n/ac требуют обратную совместимость с радиомодулями 802.11a и 802.11b/g. Следовательно, механизмы защиты также нужны для радиомодулей 802.11n/ac, чтобы сосуществовать с радиомодулями 802.11a/b/g. Поправка 802.11n изначально определяла *режимы защиты HT* [*HT protection modes*], которые включали RTS/CTS и CTS-to-Self, чтобы защитить передачи кадров данных 802.11n/ac. Пожалуйста, обратите внимание, что правила для режимов защиты HT [*HT protection modes*] также применимы для любых радиомодулей 802.11ac (VHT), а не только для радиомодулей 802.11n (HT).

### Режимы Защиты HT(0–3)

Чтобы гарантировать обратную совместимость со старыми радиомодулями 802.11a/b/g, точки доступа 802.11n/ac могут сигнализировать другим станциям 802.11n/ac когда использовать один из четырех режимов защиты HT. Как ранее упоминалось, защита HT также используется для радиомодулей VHT. Поле в кадре маяк, поле "HT Protection" (HT Защита), имеет четыре возможные установки от 0 до 4. Почти также как точки доступа ERP (802.11g), режимы защиты могут динамически меняться/переключаться, в зависимости от устройств, находящихся поблизости, или ассоциированных с точкой доступа 802.11n/ac. Механизмы защиты, которые используются, - это RTS/CTS, CTS-to-Self, Dual-CTS, или другие методы защиты. Четыре режима защиты:

**Режим 0 [Mode 0]— Режим Зеленое поле (Никакой защиты) [Greenfield (No Protection) Model]** Этот режим называется *Зеленым полем* [*Greenfield*], потому что используются только радиомодули HT. Все клиентские станции HT должны также иметь одинаковые рабочие характеристики. Если базовый состав сервиса HT является 20МГц BSS, все станции должны поддерживать 20МГц. Если базовый состав сервиса - это 20/40 МГц BSS, то все станции должны поддерживать 20/40. Если эти условия выполнены, то никакой защиты не нужно.

**Режим 1 [Mode 1]—Режим Защиты Не Участника HT [HT Nonmember Protection Model]** В этом режиме, все станции в BSS должны быть HT станциями. Механизмы защиты активируются когда услышана не-HT [non-HT] клиентская станция или не-HT [non-HT] точка доступа, которая не является участником BSS. Например, HT ТД и станции могут передавать на 40 МГц HT канале. Механизмы защиты активируются, если обнаружено, что не-HT [non-HT] 802.11a точка доступа или клиентская станция будет передавать в 20 МГц пространстве, которое инфицирует с первичным [primary] или вторичным [secondary] каналом 40МГц HT канала.

**Режим 2 [Mode 2]—Режим Защиты HT 20Мгц [HT 20 MHz Protection Mode]**

В этом режиме все станции в BSS должны быть HT станциями, и ассоциированы с 20/40 МГц точкой доступа. Если только-20 МГц ассоциируется с ТД 20/40МГц, то должна быть использована защита. Другими словами, HT станции с поддержкой 20/40 должны использовать защиту, когда передает на 40 МГц канале, для того чтобы предотвратить передачу только-20МГц HT станций в то же самое время.

**Режим 3 [Mode 3]—Не-НТ Смешанный Режим [Non-HT Mixed Mode]** Этот режим защиты используется, когда один или более не-НТ [non-HT] станций ассоциированы с НТ точкой доступа. Базовый состав сервиса НТ может быть как 20МГц , так и 20/40 МГц. Если какой-нибудь радиомодуль 802.11a/b/g ассоциирован с BSS, то будет использоваться защита. Режим 3 [Mode 3] вероятно будет наиболее распространенным режимом защиты , потому что большинство базовых составов сервиса вероятно будут иметь устаревшие устройства 802.11a/b/g в своем составе.

## Сертификация Wi-Fi Альянса

Wi-Fi Альянс управляет сертификационной программой производителей для 802.11n, называемой *СЕРТИФИЦИРОВАННЫЙ Wi-Fi n* [*Wi-Fi CERTIFIED n*], вместе с сертификацией для 802.11ac, называемой *СЕРТИФИЦИРОВАННЫЙ Wi-Fi ac* [*Wi-Fi CERTIFIED ac*]. СЕРТИФИЦИРОВАННЫЕ Wi-Fi n устройства относятся к поколению Wi-Fi 4 продуктов. СЕРТИФИЦИРОВАННЫЕ Wi-Fi ac устройства относятся к поколению Wi-Fi 5 продуктов. Обе эти сертификации тестируют продукты на обязательные [mandatory] и optionalные [optional] характеристики базового уровня, как описано в Таблице 10.7. Все сертифицированные продукты должны также поддерживать и механизмы поддержки качества сервиса Wi-Fi Мультимедиа(WMM) [Wi-Fi Multimedia (WMM) quality-of-service (QoS) mechanisms] и механизмы безопасности WPA/WPA2.

Большинство ТД уровня предприятия, которые поддерживают 802.11ac, имеют два радиомодуля: радиомодуль 2,4ГГц и радиомодуль 5ГГц. Поскольку 802.11ac работает только в частотах 5ГГц, 5ГГц радиомодуль будет тестируться, используя требования СЕРТИФИЦИРОВАННОГО Wi-Fi ac, а 2,4ГГц радиомодуль будет тестируться с использованием требований СЕРТИФИЦИРОВАННЫЙ Wi-Fi n. Обратите внимание, что устройства 802.11ac тестируются, чтобы гарантировать совместимость с ранними технологиями, которые работают в частотах 5 ГГц, которые включают 802.11n и 802.11a.

**ТАБЛИЦА 10.7** Базовые требования СЕРТИФИЦИРОВАННОГО Wi-Fi n

Характеристика	Объяснение	Тип
Поддержка двух пространственных потоков	Требуется, чтобы точки доступа передавали и принимали, как минимум, два пространственных потока. Требуется, чтобы клиентские станции передавали и принимали, как минимум, один пространственный поток.	Обязательная
Поддержка трех пространственных потоков	Точки доступа и клиентские станции должны быть способны передавать и принимать три пространственных потока.	Опциональная (испытывается, если внедрена)

Характеристика	Объяснение	Тип
Поддержка A-MPDU и A-MSDU в режиме приема; поддержка A-MPDU и A-MSDU в режиме передачи.	Требуется для всех устройств. Уменьшает служебную информацию MAC уровня.	Режим приема - обязательный
Поддержка Блокового ACK	Требуется для всех устройств. Посыпает один кадр Block ACK, чтобы подтвердить несколько полученных кадров.	Обязательная
Работа 2,4 ГГц	Устройства могут быть только 2,4ГГц, только 5 ГГц, или двух диапазонные. По этой причине, обе полосы частот перечислены как опциональные.	Опциональная (испытывается, если внедрена)
Работа 5 ГГц	Устройства могут быть только 2,4ГГц, только 5 ГГц, или двух диапазонные. По этой причине, обе полосы частот перечислены как опциональные.	Опциональная (испытывается, если внедрена)
Одновременная работа в 2,4 ГГц и 5 ГГц полосах	Этот режим проверяется только для ТД. ТД, способные работать в обоих полосах, сертифицируются как "одновременная двухдиапазонная" ["concurrent dual-band."]	Опциональная (испытывается, если внедрена)
40 МГц каналы в 5ГГц полосе	Объединение двух соседних 20МГц каналов, чтобы создать один 40МГц канал. Обеспечивает удвоение ширины полосы частот.	Опциональная (испытывается, если внедрена)
20/40 МГц механизмы сосуществования в 2,4 ГГц полосе.	Если ТД поддерживает 40 МГц каналы в 2,4 ГГц полосе, то требуются механизмы сосуществования. По умолчанию, размер канала в 2,4ГГц - 20Мгц	Опциональная (испытывается, если внедрена)
Преамбула Зеленого поля [Greenfield preamble]	Преамбула Зеленого поля не может быть прочитана устаревшими станциями. Преамбула Зеленого поля улучшает эффективность сетей 802.11n без устаревших устройств.	Опциональная (испытывается, если внедрена)
Короткий защитный интервал (short GI), 20 и 40 МГц	Короткий защитный интервал [short GI] это 400 наносекунд, традиционный GI - 800 наносекунд. Улучшает скорость передачи данных на 10 процентов.	Опциональная (испытывается, если внедрена)
Пространственно-временное блочное кодирование [Space-time block coding (STBC)]	Улучшает прием путем кодирования потоков данных блоками по нескольким антеннам. Точки доступа могут быть сертифицированы для STBC.	Опциональная (испытывается, если внедрена)
Режим Дуплицирования в HT [HT Duplicate mode]	Позволяет ТД отправлять одни и те же данные одновременно по каждому 20МГц каналу внутри объединенного 40МГц канала.	Опциональная (испытывается, если внедрена)

В июне 2013 года, до принятия поправки 802.11ac, Wi-Fi Альянс опубликовал свою программу сертификации производителей для 802.11ac, СЕРТИФИЦИРОВАННЫЙ Wi-Fi ac [Wi-Fi CERTIFIED ac]. Продукты 802.11ac тестируются и на обязательные и на опциональные характеристики базового уровня, перечисленные в Таблице 10.8. Как продукты СЕРТИФИЦИРОВАННЫЙ Wi-Fi n [Wi-Fi CERTIFIED], так и продукты САРТИФИЦИРОВАННЫЙ Wi-Fi ac [Wi-Fi CERTIFIED ac] должны поддерживать и механизмы качества сервиса Wi-Fi Мультимедиа (WMM), и механизмы безопасности WPA2. В отличии от СЕРТИФИЦИРОВАННЫХ Wi-Fi n устройств, СЕРТИФИЦИРОВАННЫЕ Wi-Fi ac устройства не работают в обоих частотных полосах 2,4ГГц и 5ГГц. СЕРТИФИЦИРОВАННЫЕ Wi-Fi ac устройства работают только в 5ГГц полосе частот. Как ранее упоминалось, это связано с ограниченным частотным диапазоном, доступном в 2,4 ГГц ISM полосе. Следовательно, СЕРТИФИЦИРОВАННЫМ Wi-Fi ac устройствам нужно только быть обратно совместимыми с 5ГГц сертифицированными устройствами 802.11a/n.

**ТАБЛИЦА 10.8** Требования базового уровня СЕРТИФИЦИРОВАННОГО Wi-Fi ac

Характеристика	Обязательно	Опционально
Ширина канала	20, 40, 80 МГц	80+80, 160 МГц
Схема кодирования и модуляции	MCS 0–7	MCS 8, 9
Пространственные потоки	Один для клиентов, два для ТД	От двух до восьми
Защитный Интервал	И Длинный (800 наносекунд) и Короткий (400 наносекунд)	
Обратная связь формирования луча		Ответ на исследование при формировании луча
Пространственно-временное блочное кодирование (STBC)		Передача и прием STBC
Низкая Плотность Проверок на Четность [Low-density parity check (LDPC)]		Передача и прием LDPC
Многопользовательское MIMO		До четырех пространственных потоков на клиента, используя один и тот же MCS

## Итого

В этой главе вы узнали историю поправок 802.11n и 802.11ac, и как Wi-Fi Альянс сертифицирует совместимость. Мы также обсудили все методы, используемые радиомодулями НТ и ВНТ, чтобы увеличить пропускную способность и расстояние на Физическом уровне. В дополнение к улучшениям PHY, эти радиомодули используют механизмы MAC уровня, чтобы улучшить пропускную способность и управление питанием. Наконец, мы обсудили различные режимы работы, которые используются для механизмов защиты и существования со старыми устаревшими технологиями 802.11a/b/g. Поскольку стандарт 802.11ac разработан для работы только в 5 ГГц диапазоне частот, точки доступа 802.11ac с двумя радиомодулями продолжают поддерживать 802.11n в диапазоне частот 2,4 ГГц некоторое время. Если вам интересно узнать больше о 802.11ac, мы рекомендуем вам прочитать 802.11 ac: Руководство по Выживанию, Мэттью Гаст (O'Reilly Media, 2013 год) [*802.11ac: A Survival Guide*, by Matthew Gast (O'Reilly Media, 2013)]. Мэттью проделал великолепную работу по объяснению основных технологий, которые составляют 802.11ac, в подробном и лаконичном формате.

## Темы Экзамена

**Определить разницу между MIMO и SISO.** Понимать, что SISO устройства используют только одну радиотехническую цепь, в то время как MIMO системы используют несколько радиоцепей.

**Определить различия между 802.11n и 802.11ac.** Понимать, чем 802.11ac похожа и чем отличается от 802.11n. Объяснить, почему 802.11ac реализована только в полосе 5ГГц.

**Понимать разнесение MIMO.** Объяснить методы разнесения множественной передачи и приема, таких как пространственное мультиплексирование, комбинация максимального отношения, пространственно-временное блочное кодирование, разнесение с циклическим сдвигом и формирование луча при передаче. Понимать, как разнесение MIMO использует преимущества многолучевого распространения.

**Объяснить разницу между SU-MIMO и MU-MIMO.** Объяснить сколько пространственных потоков поддерживается 802.11ac вместе с дополнительными ресурсами, необходимыми для внедрения большего количества пространственных потоков. Объяснить технологические различия между отправкой SU-MIMO сигнала и MU-MIMO сигнала.

**Объяснить MU-MIMO.** Объяснить процесс и условия MU-MIMO, при которых оно будет наиболее успешно. Объяснить, как формирование луча делает это возможным. Объяснить требования для добавления пространственных потоков. Объяснить как QoS реализован в среде MU-MIMO.

**Описать явное формирование луча.** Описать взаимодействие между ТД и клиентом для выполнения явного формирования луча. Описать преимущества явного формирования луча.

**Понимать каналы 20 МГц, 40 МГц, 80 МГц, и 160 МГц.** Понимать различия между 20 МГц, 40 МГц, 80 МГц, и 160 МГц каналами. Объяснить, что 160МГц канал в действительности – это два 80МГц канала. Объяснить, как радиомодули 802.11ac динамически переключаются на более узкие каналы, если более широкие каналы не доступны. Описать важность выбора первичного канала для каждой ширины канала.

**Объяснить защитный интервал.** Описать как защитный интервал компенсирует межсимвольную интерференцию. Обсудить использование и 800, 400 наносекундных GI.

**Понимать модуляцию и схемы кодирования.** Объяснить, как используются схемы кодирования и модуляции (MCS) для определения скоростей передачи данных. Объяснить все переменные, которые могут повлиять на скорости передачи данных.

**Объяснить HT/VHT PPDU форматы.** Описать различия между устаревшим не-HT[non-HT], Смешанным HT, и VHT PPDU.

**Понимать улучшения HT MAC.** Объяснить, как используется агрегация кадров для увеличения пропускной способности на MAC подуровне. Определить новые методы управления питанием, используемые радиомодулями HT/ VHT.

**Объяснить режимы защиты HT.** Описать различия между режимами защиты 0-3. Понимать, что эти режимы защиты используются и для HT, и для VHT радиомодулей.

**Понимать 64-QAM и 256-QAM.** Объяснить, чем 256-QAM похожа и чем отличается от 64-QAM. Описать значение диаграмм созвездий и за, и против более плотного 256-QAM.

## Контрольные вопросы

1. Какой из перечисленных методов модуляции поддерживается в 802.11ac? (Выберите все, что применимо.)

  - A. BPSK
  - B. BASK
  - C. 1024-QAM
  - D. 64-QAM
  - E. 256-QAM
2. Как система МИМО может увеличить пропускную способность на Физическом уровне? (Выберите все, что применимо.)

  - A. Пространственное мультиплексирование [Spatial multiplexing]
  - B. A-MPDU
  - C. Формирование луча по передаче [Transmit beamforming]
  - D. 40 МГц каналы
3. Какой метод управления питанием [power-management method], определенный поправкой 802.11n, сберегает энергию путем выключения всех, кроме одного, радиомодулей?

  - A. A-MPDU
  - B. Защита Энерго Сбережения [Power Save protection]
  - C. PSMP
  - D. Энерго Сбережение Пространственного Мультиплексирования [SM power save]
  - E. Режим PS [PS mode]
4. Защитный интервал используется в качестве буфера для компенсации какого типа интерференции?

  - A. Соканальная интерференция [Co-channel interference]
  - B. Интерференция смежных сот [Adjacent cell interference]
  - C. Радиоволновая интерференция [RF interference]
  - D. HT Интерференция [HT interference]
  - E. Межсимвольная интерференция [Intersymbol interference]
5. Какая из следующих ширин каналов поддерживается в 802.11ac? (Выберите все, что применимо.)

  - A. 20 МГц
  - B. 40 МГц
  - C. 80 МГц
  - D. 80+80 МГц
  - E. 160 МГц

- 6.** Что может использовать радиомодуль 802.11n (HT), чтобы увеличить пропускную способность на MAC подуровне Канального уровня [Data-Link layer]? (Выберите все, что применимо.)
- A.** A-MSDU
  - B.** A-MPDU
  - C.** Защитный интервал [Guard interval]
  - D.** Блоковые ACKs [Block ACKs]
  - E.** Пространственное мультиплексирование [Spatial multiplexing]
- 7.** Какая из следующих технологий является частью явного формирования луча [beamforming]? (Выберите все, что применимо.)
- A.** Канальное исследование [Channel sounding]
  - B.** Матрица обратной связи [Feedback matrix]
  - C.** Матрица исследования [Sounding matrix]
  - D.** Управляющая матрица [Steering matrix]
  - E.** Пустой пакет данных [Null data packet]
  - F.** Канальная матрица [Channel matrix]
- 8.** Радиомодуль 3×3:2 MIMO сколько может передавать и принимать уникальных потоков данных?
- A.** Два
  - B.** Три
  - C.** Четыре
  - D.** Пять
  - E.** Нисколько—потоки являются не уникальными данными.
- 9.** Название способности, не определенной для A-MPDU.
- A.** Множественные категории доступа QoS [Multiple QoS access categories]
  - B.** Независимое шифрование данных полезной нагрузки [Independent data payload encryption]
  - C.** Индивидуальные MPDU, имеющие один и тот же адрес получателя [Individual MPDUs having the same receiver address]
  - D.** Агрегация MPDU [MPDU aggregation]
- 10.** Какие режимы защиты HT [HT protection modes] разрешены только для ассоциации клиентов 802.11a/g с точкой доступа 802.11ac? (Выберите все, что применимо.)
- A.** Режим 0 - режим Зеленого поля [Mode 0—Greenfield mode]
  - B.** Режим 1 - Режим защиты не участника HT [Mode 1—HT nonmember protection mode]
  - C.** Режим 2 - Режим защиты 20МГц HT [Mode 2—HT 20 MHz protection mode]
  - D.** Режим 3 - Смешанный режим HT [Mode 3—HT Mixed mode]
- 11.** Какие из этих выражений о 40МГц каналах верны? (Выберите все, что применимо.)
- A.** Кадры управления и контрольные кадры 802.11 передаются только в первичном [primary] канале.

- B.** Кадры 802.11n/ac могут быть отправлены вместе по первичному и вторичному каналам.
  - C.** Кадры управления и контрольные кадры 802.11 передаются только по вторичному [secondary] каналу.
  - D.** Кадры данных 802.11, отправленные клиентом 802.11g, отправляются по вторичному каналу.
  - E.** Кадры данных 802.11, отправленные клиентом 802.11g, отправляются по первичному каналу.
- 12.** MIMO радиомодули используют какой механизм для разнесения передачи? (Выберите все, что применимо.)
- A.** Комбинация максимального отношения (MRC)
  - B.** Расширение спектра прямой-последовательностью (DSSS)
  - C.** Пространственно-временное блочное кодирование (STBC)
  - D.** Разнесение с циклическим сдвигом (CSD)
  - E.** Пространственное мультиплексирование (SM)
- 13.** Радиомодули 802.11n (HT) обратно совместимы с каким из следующих типов радиомодулей 802.11? (Выберите все, что применимо.)
- A.** Радиомодули 802.11b (HR-DSSS)
  - B.** Радиомодули 802.11a (OFDM)
  - C.** Устаревшие радиомодули 802.11 (FHSS)
  - D.** Радиомодули 802.11g (ERP)
- 14.** Сколько модуляций и схем кодирования определено в 802.11ac?
- A.** 8
  - B.** 10
  - C.** 64
  - D.** 77
  - E.** 256
- 15.** Какой диапазон MCS 802.11ac определяет все MCS, которые обязательны для Wi-Fi сертификации?
- A.** MCS 0–2
  - B.** MCS 0–4
  - C.** MCS 0–6
  - D.** MCS 0–7
  - E.** MCS 0–8
  - F.** MCS 0–9
- 16.** Брэйдон, консультант по БЛВС, рекомендовал, чтобы в новой сети 802.11n/ac 40МГц каналы использовали только в полосах 5ГГц U-NII. Почему он рекомендовал, чтобы 40МГц каналы использовались только в 5 ГГц и не использовались в 2,4ГГц?
- A.** Радиомодули HT/ VHT не требуют DFS и TPC в 5 ГГц полосах.
  - B.** Радиомодули HT/ VHT получают лучший диапазон, используя TxBF в полосах 5ГГц.
  - C.** 40 МГц каналы не масштабируются в полосе 2,4 ГГц ISM.
  - D.** 5 ГГц VHT радиомодули менее дорогие, чем 2,4 ГГц HT радиомодули.

- 17.** Радиомодули 802.11ac (VHT) обратно совместимы с каким из следующих типов технологий 802.11? (Выберите все, что применимо.)
- A.** 802.11b (HR-DSSS)
  - B.** 802.11a (OFDM)
  - C.** 802.11g (ERP)
  - D.** 802.11n (HT)
- 18.** Какой из этих методов разнесения MIMO по приему полезен при приеме входящих передач от SISO радиомодуля?
- A.** Пространственно-временное блочное кодирование (STBC)
  - B.** Комбинация максимального отношения (MRC)
  - C.** Формирование тучи на передаче (TxBF)
  - D.** Пространственное мультиплексирование (SM)
- 19.** Какой механизм уровня PHY может быть использован для увеличения пропускной способности для радиомодулей HT/ VHT в чистой радиосреде с минимальными отражениями и низким многолучевым распространением?
- A.** Комбинация максимального отношения
  - B.** 400-наносекундный защитный интервал
  - C.** Переключаемое разнесение
  - D.** Пространственное мультиплексирование
  - E.** Пространственное разнесение
- 20.** Сколько максимально возможных пространственных потоков для клиента определяет поправка 802.11ac?
- A.** Один
  - B.** Два
  - C.** Четыре
  - D.** Восемь



# Глава 11



# Архитектура БЛВС

---

В ЭТОЙ ГЛАВЕ ВЫ УЗНАЕТЕ О СЛЕДУЮЩЕМ:

✓ **Клиентские устройства БЛВС**

- Форм факторы радиомодулей 802.11
- Чипсеты радиомодулей 802.11
- Клиентские утилиты

✓ **Плоскости Управления, Контроля и Данных**

- Плоскость управления
- Плоскость контроля
- Плоскость данных

✓ **Архитектура БЛВС**

- Архитектура автономной БЛВС
- Централизованные системы управления сетью
- Централизованная архитектура БЛВС
- Распределенная архитектура БЛВС
- Гибридная архитектура БЛВС

✓ **Специальная инфраструктура БЛВС**

- Маршрутизаторы БЛВС филиалов предприятий
- БЛВС точки доступа с поддержкой взаимосвязности(mesh)
- Мосты БЛВС
- Системы позиционирования реального времени
- VoWiFi

✓ **Облачные сети**



✓ **Программируемый интерфейс приложения**  
[Application programming interface]

- Транспорт и форматы данных
  - БЛВС API [WLAN APIs]
  - Типовые приложения

✓ **Управление инфраструктурой**

- Протоколы управления



В Главе 7 "Топологии Беспроводной ЛВС" мы обсудили различные топологии БЛВС 802.11. Вы узнали, что станции [stations] и клиента, и точки доступа могут быть организованы в сервисный состав 802.11 [802.11 service set], чтобы обеспечить беспроводной доступ к другой среде.

В этой главе мы обсуждаем несколько устройств, которые могут быть использованы в топологиях 802.11. Существует большой выбор радио карт для клиентских станций, которые могут быть использованы в настольных ПК, ноутбуках, смартфонах, планшетах, и т.д.

Мы также обсуждаем три логические плоскости работы сети, и где они применяются в БЛВС. Эта глава дает обзор множества различных архитектур БЛВС, которые доступны сегодня. Мы также исследуем развитие инфраструктурных устройств БЛВС за несколько лет. Мы также раскрываем назначение многих специальных устройств БЛВС, которые существуют на сегодняшнем рынке Wi-Fi.

## Клиентские Устройства БЛВС

Главное оборудование в *сетевой интерфейсной карте* Wi-Fi [*network interface card (NIC)*] – полудуплексный радиочастотный приемопередатчик, который может существовать во множестве аппаратных форматах и чипсетах (наборах микросхем). Все клиентские Wi-Fi NIC требуют определенный драйвер, чтобы взаимодействовать с операционной системой, а также программы-утилиты для взаимодействия с конечным пользователем. Wi-Fi радиомодули Ноутбуков могут работать с Windows, Linux, ChromeOS, и macOS, хотя они требуют разные драйвера и клиентское программное обеспечение для каждой операционной системы. Драйвера радиомодулей многих производителей могут уже быть включены в операционную систему, но часто более новые радиомодули требуют установку новых драйверов, или могут стать лучше от установки более свежих драйверов. Многие производители обеспечивают автоматический онлайн метод обновления драйверов; однако, некоторым драйверам может понадобится ручная установка в операционную систему. Первое поколение драйверов Wi-Fi радиомодулей часто бывают с ошибками(багами). Администратор или пользователь должны всегда убеждаться, что установлено наиболее актуальное поколение драйверов. Большой процент проблем с Wi-Fi решается путем простого обновления клиентских драйверов БЛВС.

В программном интерфейсе конечный пользователь может настроить сетевую карту (NIC), чтобы стать участником БЛВС, используя конфигурационные настройки, которые относятся к идентификации, безопасности и производительности. Эти клиентские утилиты могут быть собственным программным обеспечением производителя или объединенным программным интерфейсом, встроенным в операционную систему.

Далее, мы обсудим различные форматы сетевых интерфейсных радиокарт [radio NIC], используемые чипсеты (наборы микросхем), и программные клиентские утилиты (инструменты).

## Форм Факторы Радиомодулей 802.11

Радиомодули 802.11 используются и в клиентских NIC и точках доступа.

Следующие разделы фокусируются главным образом на том, как радиомодули Wi-Fi могут быть использованы в качестве клиентских устройств. Радиомодули 802.11 производятся во множестве *форм факторов [form factors]*, что означает, что NIC (сетевые карты) имеют разные формы и размеры. Много форм факторов радиомодулей Wi-Fi, таких как USB, подразумевают использование в качестве дополнительного [add-on] внешнего устройства, хотя большая часть Wi-Fi устройств теперь использует внутренние или интегрированные форм факторы.

### Внешние Wi-Fi радиомодули

Когда БЛВС 802.11 были впервые развернуты, у вас была единственная опция при покупке клиентской сетевой карты (NIC) 802.11 – стандартный адаптер PC Card, который был периферией для ноутбуков. Форм фактор PC Card был разработан Международной Ассоциацией Карт Памяти Персональных Компьютеров [Personal Computer Memory Card International Association (PCMCIA)]. Три устаревших адаптера PCMCIA, также известных как PC Card, показаны на Рисунке 11.1. Радио карта PCMCIA могла быть использована в любом ноутбуке и ручном устройстве, которое имело слот PC Card. Большинство PC card имеют только внутренние интегрированные антенны, в то время как у других есть и внутренние антенные и внешние разъемы. Ноутбуки больше не производятся со слотами PC Card, и радиомодули PCMCIA стали невостребованными.

**РИСУНОК 11.1** Адаптер PCMCIA/PC card

Любезно предоставлено Cisco Systems, Inc. Использование без разрешения не допускается.



В итоге, радиомодули других форм факторов появились на рынке, включая формат *ExpressCard*. ExpressCard был аппаратным стандартом, который заменил карты PCMCIA. Большинство производителей ноутбуков заменили слоты PCMCIA на меньшие слоты ExpressCard.

Были два периферийных форм фактора радиомодулей *Secure Digital (SD)* и *CompactFlash (CF)*, которые изначально использовались с ручными персональными цифровыми ассистентами [personal digital assistants (PDAs)]. Эти радиомодули обычно

требовали очень мало энергии и были меньше, чем спички-книжки. Использование форматов SD и CF с ручными устройствами быстро стало невостребованным, из-за того, что в ручные устройства интегрировали радиомодули 802.11 встраиваемых форм факторов.

Мы обсудили несколько форм факторов Wi-Fi радиомодулей, которые могут быть использованы в качестве внешних радиомодулей с ноутбуками и другими мобильными устройствами. Однако, радиомодули 802.11 *Универсальной Последовательной Шины* [*Universal Serial Bus (USB)*] остаются наиболее популярным выбором для внешних Wi-Fi радиомодулей, потому что почти у всех компьютеров есть USB порты. USB технология предоставляет простоту установки и не требует внешний источник питания. USB радиомодули 802.11 существуют или в форме небольших вставляемых устройств типа донгл[*dongle*] (см. Рисунок 11.2), или в качестве внешнего проводного USB устройства с отдельным разъемом для USB кабеля. Устройства донгл [dongle] компактны и переносимы для использования с ноутбуками, а внешние устройства могут быть подключены к настольному компьютеру USB кабелем, и установлены на стол для лучшего приема.

**РИСУНОК 11.2** USB радиомодуль 802.11



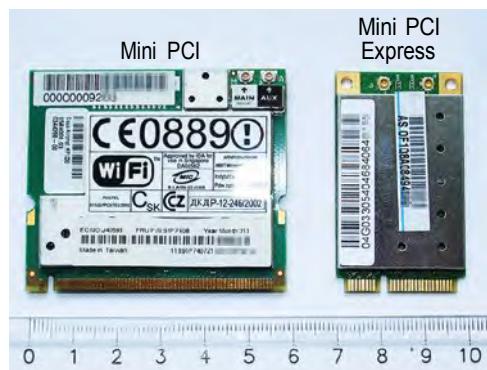
Радиомодули 802.11n/ac доступны в обоих форм факторах USB 2.0 и USB 3.0 и могут работать в обоих полосах частот 2,4ГГц и 5ГГц. Учтите, что существуют некоторые недостатки при использовании радиомодулей USB форм фактора. Технология USB 2.0 определяет скорость передачи данных только до 480Мбит/с, что будет ограничивать доступные скорости передачи данных 802.11. Технология USB 3.0 потенциально определяет скорость передачи данных до 5Гбит/с. Wi-Fi радиомодули USB 3.0 могут, следовательно, использовать преимущества более высоких скоростей передачи данных 802.11n/ac. Пожалуйста, учтите, что схемы в некоторых устройствах USB 3.0 вызывают радиоинтерференцию в 2,4ГГц полосе. Было показано, что устройства USB 3.0 различных типов повышают уровень шума на 5-20дБ, что может стать причиной серьезных проблем производительности с внутренними радиомодулями 802.11 в ноутбуках.

## Внутренние Wi-Fi радиомодули

Много лет, внешние Wi-Fi радиомодули были нормой, потому что в ноутбуках не было внутренних Wi-Fi радиомодулей. Теперь ноутбуки и другие мобильные устройства включают в себя внутренние Wi-Fi радиомодули.

Формат внутреннего радиомодуля, который использовался изначально, был *Mini PCI*. Mini PCI был вариацией технологии шины Взаимного Соединения Компонентов Периферии [Peripheral Component Interconnect (PCI)] и был разработан для использования в основном в ноутбуках. Радиомодуль Mini PCI часто использовался внутри точек доступа, и был также основным типом радиомодулей, используемых производителями в качестве внутреннего беспроводного адаптера 802.11 внутри ноутбуков. Форм фактор технологии шины следующего поколения – это меньший по размеру *Мини PCI Экспресс* [*Mini PCI Express*], и даже еще меньший *Половинный Мини PCI Экспресс* [*Half Mini PCI Express*]. Сегодня почти невозможно купить новый ноутбук, у которого нет внутреннего Mini PCI или Mini PCI Express радиомодуля, изображенных на Рисунке 11.3. Радиокрты Mini PCI или Mini PCI Express обычно устанавливаются снизу ноутбука, и подключаются к небольшим антеннам, которые установлены вдоль края монитора ноутбука.

**РИСУНОК 11.3** Mini PCI и Mini PCI Express радиомодули





## Пример из Реальной Жизни

### Преимущества Использования Внешнего USB Радиомодуля с Ноутбуком

Хотя радиомодули Mini PCI, Mini PCI Express, и Half Mini PCI Express являются вынимаемыми из некоторых ноутбуков, нет никакой гарантии, что любой из этих форм факторов будет работать в ноутбуке другого производителя. Преимущество использования USB Wi-Fi адаптеров в том, что их можно переносить и использовать в разных ноутбуках. Кроме того, ноутбуки со старыми внутренними радиомодулями 802.11 могут быть мгновенно усовершенствованы до более новой технологии 802.11 за низкую стоимость USB радиомодуля. Также, инженеры БЛВС обычно используют USB радиомодуль, когда запускают программный анализатор протокола 802.11 и/или приложение по радио обследованию. Эти приложения часто требуют специальный драйвер для радиомодуля 802.11, который ставится поверх и/или конфликтует с драйвером оригинального радиомодуля. Использование независимого и внешнего Wi-Fi радиомодуля для поиска и устранения проблем и для радио обследования является общепринятой практикой, так что драйвер внутреннего Wi-Fi радиомодуля остается нетронутым.

## Мобильные устройства

Мы в основном обсудили различные типы форматов сетевых карт (NIC)-радиомодулей 802.11, которые используются с ноутбуками. Радиомодули 802.11 также используются во многих других типах ручных устройств, таких как смартфоны, планшеты, сканеры штрихкодов, и VoWiFi телефоны. Сканеры штрихкодов, такие как мобильное устройство Honeywell, показанное на Рисунке 11.4, уже много лет используют радиомодули 802.11.

**Р И С У Н О К 11.4** Сканер штрихкодов

Любезно предоставлено Honeywell



Хотя старые ручные устройства использовали некоторые из ранее упомянутых форм факторов, производители большинства ручных устройств используют радиомодуль 802.11 встраиваемого форм фактора [embedded form factor] (обычно одномикросхемный форм фактор [chip form factor], который встроен в материнскую плату устройства.). Рисунок 11.5 показывает одномикросхемный Wi-Fi радиомодуль компании Broadcom, который находится внутри некоторых моделей Apple iPhone. Почти все мобильные устройства, такие как смартфоны и планшеты, используют одномикросхемный форм фактор [single chip form factor], который встраивается в материнскую плату устройства. Встраиваемые радиомодули часто используют комбинированные микросхемы (чипсеты)[combo chipset] для радиомодулей Wi-Fi и Bluetooth.

**РИСУНОК 11.5** Встраиваемый радиомодуль 802.11



В течении многих лет, большинство людей думало только об использовании ноутбуков для подключения к Wi-Fi. С появлением смартфонов и планшетов, произошел взрыв численности клиентских ручных мобильных устройств. Последние годы, число мобильных устройств, подключенных к БЛВС предприятий, превзошло число ноутбуков, подключенных к тем же самим БЛВС предприятий. Фирма по исследованию технологий 650 Групп [650 Group ([www.650group.com](http://www.650group.com))] оценивает, что к 2025 году, число используемых смартфонов, планшетов, ПК и периферии достигнет свыше 11 миллиардов единиц по всему миру.

Теперь пользователи ожидают подключение к Wi-Fi с многочисленных мобильных устройств в дополнение к своим ноутбукам. Из-за распространения персональных мобильных устройств, политика *приноси свое собственное устройство* [*bring your own device (BYOD)*] часто нуждается в определении того, как персональные устройства сотрудников могут получить доступ к корпоративной БЛВС. Решение по управлению мобильными устройствами [*mobile device management (MDM)*] может также быть необходимым для допуска персональных мобильных устройств и устройств самой компании в БЛВС. Стратегии BYOD и решения MDM обсуждаются более детально в Главе 18 "Приноси Свое Собственное Устройство (BYOD) и Гостевой Доступ".

## Носимые устройства

Еще одна большая технологическая тенденция - носимые (одеваемые) компьютеры, в англоязычной среде называемые *wearables*, в русскоязычной среде - умные носимые устройства. Носимые вычислительные устройства одеваются на тело и/или одежду. Носимые устройства означают обеспечение постоянного взаимодействия между человеком и компьютером, и носимые устройства становятся расширением тела пользователя или сознания. Хотя концепция носимых компьютеров не нова, носимые устройства со

встроенным Wi-Fi радиомодулями начали искать свой путь на рынке. Пример носимых компьютеров включает умные часы, браслеты, датчики упражнений, и очки.

Почти также, как и со смартфонами и планшетами, пользователи могут захотеть подключиться к БЛВС компании своими персональными носимыми вычислительными устройствами. Теперь появились новые вызовы - как ИТ администраторам управлять политиками подключения и доступа носимых устройств к корпоративной БЛВС. Кроме того, носимые устройства имеют потенциал для многочисленных приложений в вертикалях предприятий, таких как здравоохранение [healthcare] и розница[retail]. 650 Групп планирует, что число поставленных носимых устройств вырастет с 1 миллиарда в 2017 году до примерно 5 миллиардов в 2025 году.

## Интернет вещей

Когда говорят о RFID устройствах, фразу Интернет Вещей [*Internet of Things (IoT)*] обычно приписывают Кевину Эштону [Kevin Ashton]:

[www.rfidjournal.com/articles/view?4986](http://www.rfidjournal.com/articles/view?4986)

Годами, большая часть данных, генерируемых в Интернете, создавалась людьми. Теория Интернета Вещей [*Internet of Things*] в том, что в будущем, большой объем данных, генерируемых в Интернете, может создаваться датчиками, мониторинговыми устройствами, и машинами. Следует отметить, что радиомодули 802.11 сетевых карт (NIC), используемые в качестве клиентских устройств, начали появляться во многих типах машин и решений. Радиомодули Wi-Fi уже присутствуют в игровых устройствах, стерео системах, и видеокамерах. Производители техники уже размещают Wi-Fi NICs в стиральных машинах, холодильниках, и автомобилях. Использование Wi-Fi радиомодулей в датчиках и мониторинговых устройствах также, как и RFID, имеет много применений в многочисленных вертикальных рынках предприятий

Фирма по исследованию технологий 650 Групп [650 Group] оценивает, что к 2025 году, число беспроводных подключенных IoT устройств будет 59 миллиардов единиц по всему миру, далеко превышая ожидаемые 28 миллиардов ПК, планшетов, смартфонов, и других подключенных персональных устройств. Может это быть началом самосознательного Скайнет [Skynet], предсказанного фильмом *Терминатор* [*Terminator*]? Все шутки в сторону, большая часть IoT устройств будет вероятнее всего подключена к Интернету с помощью Wi-Fi радиомодуля. Еще раз, появляются новые задачи; ИТ администраторы должны управлять политиками регистрации, доступа, и безопасности IoT устройств, подключающихся к корпоративной БЛВС.

Большой объем IoT устройств с радиомодулем 802.11 на текущий момент передают только в полосе частот 2,4 ГГц. Нужно понимать, что не все IoT устройства используют Wi-Fi радиомодули. IoT устройства могут использовать другие радиотехнологии, такие как Bluetooth или Zigbee. IoT устройства также могут иметь сетевой интерфейс Ethernet в дополнение к радио интерфейсам.



## Пример из Реальной Жизни

### Как Я Узнаю Какой Тип Радиомодуля в Моем Ноутбуке или Мобильном Устройстве?

Часто, производитель ноутбуков или мобильных устройств указывает модель радиомодуля в листке спецификации ноутбука или мобильного устройства. Однако, некоторые производители могут не указать детальную спецификацию и характеристики радиомодуля. Что, если вы хотите выяснить является ли радиомодуль MIMO 1×1:1 или, может быть, MIMO 3×3:3? Поддерживает ли радиомодуль 40 МГц каналы или только 20МГц каналы? На ноутбуках, вы можете найти некоторые характеристики радиомодуля, посмотрев на драйвера радиомодуля в OS. Еще один способ идентификации Wi-Fi радиомодуля в вашем устройстве - это по FCC ID. В Соединенных Штатах, все Wi-Fi радиомодули должны быть сертифицированы государственным агентством Федеральной Комиссии по Связи (FCC). FCC поддерживает базу данных авторизованного оборудования с возможностью поиска по адресу [www.fcc.gov/oet/ea/fccid](http://www.fcc.gov/oet/ea/fccid). Вы можете ввести FCC ID вашего устройства в поисковую машину базы данных и найти документацию и картинки, предоставленные производителем в FCC. База данных FCC очень полезна в идентификации моделей Wi-Fi радиомодуля и спецификации, если информация не доступна на сайте производителя.

## Возможности Клиентского Устройства

В Главе 13 "Концепции Проектирования БЛВС" мы обсудим важность понимания возможностей клиентов, которых вы устанавливаете в среде предприятия. Мы также обсудим важность обновления клиентских устройств вашей БЛВС на более новую технологию 802.11, когда вы обновляете [upgrade] ваши точки доступа. Большинство предприятий и корпораций могут устраниТЬ множество проблем с клиентским подключением и производительностью путем обновления клиентских устройств, принадлежащих компании, прежде обновления инфраструктуры БЛВС. К сожалению, обратное часто более привычно, компании тратят много сотен или тысяч долларов на обновление технологии с новыми точками доступа, при этом продолжают устанавливать устаревшие клиенты.

Всегда помните, что у всех клиентских радиомодулей 802.11 не одинаковые характеристики. У устаревших радиомодулей 802.11b максимальная скорость передачи данных 11 Мбит/с, а у устаревших радиомодулей 802.11a/g максимальная скорость передачи данных 54Мбит/с. За последнее десятилетие производители ноутбуков, смартфонов и планшетов поставляли свои продукты с радиомодулями 802.11n/ac, которые способны дать намного большие скорости передачи данных. Теперь производители поставляют устройства с радиомодулями 802.11ax, с расширенной эффективностью. Однако, знайте, что даже современные клиентские устройства могут не иметь одинаковых характеристик. Некоторые ноутбуки высокого класса могут иметь радиомодуль 3×3:3 MIMO, но большая часть ноутбуков имеют радиомодули 2×2:2 MIMO. Также, большинство смартфонов и планшетов сейчас имеют радиомодули 2×2:2, но много старых мобильных устройств 802.11n были 1×1:1.

У нескольких первых поколений планшетных ПК и смартфонов были радиомодули 1×1:1, которые работали только в полосе частот 2,4ГГц. У большинства современных клиентов двухчастотные радиомодули 2×2:2 MIMO, которые работают в обоих полосах частот 2,4ГГц и 5 ГГц. Также, основная часть новых клиентов обычно поддерживают 40МГц каналы. Клиентские устройства с 6ГГц Wi-Fi радиомодули могут появится на рынке в начале 2021 года. Не все технологии 802.11 всегда поддерживаются на клиентах. Например: возможности 802.11k, 802.11r и 802.11v могут не поддерживаться, даже на новых клиентских устройствах.

IoT устройства с радиомодулями 802.11 обычно работают только в полосе частот 2,4ГГц, и очень часто могут применять технологии старых 802.11 микросхем (chipset), чтобы сохранить низкую цену.

## Чипсеты Радиомодулей 802.11

Группа интегральных цепей, спроектированных, чтобы работать вместе, часто выдается на рынок как *чипсет*[*chipset*] или *набор микросхем*. Существует много производителей чипсетов 802.11, которые продают свои технологии чипсетов различным производителям радиомодулей и производителям БЛВС. Устаревшие чипсеты очевидно не будут поддерживать все те же самые характеристики, что и более новые технологии чипсетов. Например, устаревшие чипсеты могут поддерживать только технологии 802.11a/b/g, в то время как более новые чипсеты (наборы микросхем) будут поддерживать технологии 802.11n/ac и 802.11ax.

Некоторые чипсеты могут поддерживать способность передавать только в полосе 2,4ГГц ISM; другие чипсеты могут передавать на 2,4ГГц или 5ГГц нелицензируемых частотах. 6 ГГц чипсеты запланированы к выходу в 2021 году. Современные чипсеты, которые поддерживают обе частоты, используются в клиентских радиомодулях 802.11n/ac и 802.11ax. Производители чипсетов включают более новые технологии 802.11 по мере их развития. Многие проприетарные технологии включены в отдельные чипсеты, и некоторые из этих технологий станут частью стандарта в будущих поправках 802.11.



Вы можете найти подробную информацию о некоторых из наиболее широко используемых Wi-Fi чипсетах и производителях радиомодулей по следующим URL: [www.qualcomm.com](http://www.qualcomm.com), [www.broadcom.com](http://www.broadcom.com), и [www.intel.com](http://www.intel.com).

## Клиентские Утилиты

Конечный пользователь должен иметь возможность настроить беспроводную клиентскую сетьевую карту (NIC). Следовательно, требуется программный интерфейс в виде *клиентских утилит* [*client utilities*]. Почти также как драйвер – это интерфейс между сетевой радиокартой [radio NIC] и операционной системой, клиентская Wi-Fi утилита – это, фактически, программный интерфейс между сетевой радиокартой [radio NIC] и вами. Программный интерфейс обычно имеет возможность создавать несколько профилей подключений. Один профиль может быть использован для подключения к беспроводной сети на работе, другой для подключения дома, а третий для подключения к хотспоту.

Настройки конфигурации для клиентской утилиты обычно включают идентификатор сервисного состава [service set identifier (SSID)], мощность передачи, настройки безопасности WPA2/WPA3, параметры качества-сервиса Wi-Fi Мультимедиа

(WMM), и настройки управления питанием. Еще один технический термин, часто используемый для клиентских утилит БЛВС в англоязычной среде – *supplicant* (в переводе означает – просящий), на русский переводится как *клиент*. Термин *supplicant* (просящий) наиболее часто используется при обсуждении безопасности 802.1X/EAP. Как упоминалось в Главе 7, некоторые клиентские сетевые карты (NIC) могут также быть настроены в режиме инфраструктуры или в режиме «на лету» [ad-hoc]. У большинства хороших клиентских утилит есть своего рода экран со статистической информацией, а также своего рода измерительный инструмент индикатора силы принимаемого сигнала [received signal strength indicator (RSSI)]. Некоторые клиентские утилиты позволяют настраивать пороги клиентского роуминга (переключения).

Существует два главных типа, или категории, клиентских утилит:

- Клиентские утилиты, интегрированные в операционную систему
- Сторонние клиентские утилиты [Third-party client utilities]

Программный интерфейс, который наиболее широко используется для настройки Wi-Fi радиомодуля – это, обычно, клиентские Wi-Fi утилиты, встроенные в операционную систему. Пользователи ноутбуков наиболее вероятно будут использовать конфигурационный интерфейс Wi-Fi сетевой карты (NIC), который является частью ОС, работающей на ноутбуке. Клиентские программные утилиты различаются в зависимости от ОС используемого ноутбука. Возможности клиентских Wi-Fi утилит также варьируются между разными версиями операционных систем. Например, клиентская утилита Windows 8 отличается от клиентской утилиты Windows 10. Клиентские утилиты старого macOS отличаются от клиентской утилиты macOS 10.15 (Catalina). Рисунок 11.6 показывает клиентскую утилиту Wi-Fi Windows 10.

**РИСУНОК 11.6** Клиентская утилита, интегрированная в ОС для Windows 10



Операционные системы ручных устройств обычно также включают своего рода клиентские Wi-Fi утилиты. Рисунок 11.7 показывает клиентский интерфейс, находящийся в Apple iOS 14.0, которая работает на iPhones.

**РИСУНОК 11.7** Интегрированная в ОС клиентская утилита для iOS 14.0



Вместо использования клиентского программного клиента [supplicant] Wi-Fi операционной системы, некоторые предприятия выбирают использование сторонних клиентских утилит, таких как SecureW2's Enterprise Client for Windows, показанной на Рисунке 11.8. Почти так же , как интегрированное в ОС клиентское программное обеспечение, сторонняя БЛВС утилита будет работать с радиокартами разных производителей, делая административную поддержку намного легче. В прошлом, сторонние клиентские утилиты часто предоставляли преимущество поддержки множества разных типов EAP, давая администратору БЛВС широкий диапазон выбора безопасности. Главный недостаток сторонних клиентских утилит в том, что они, обычно, стоят дополнительных денег. Так как интегрированные клиентские утилиты с годами стали лучше, от использования сторонних клиентских утилит потихоньку отказались.

**FIGURE 11.8** Сторонняя клиентская утилита

## Плоскости Управления, Контроля и Данных

Телекоммуникационные сети часто определяются как три логические плоскости работы:

**Плоскость Управления [Management Plane]** *Плоскость управления [management plane]* определяется административным управлением сетью, администрированием и мониторингом. Примером плоскости управления может быть любое решение по сетевому управлению, которое может быть использовано для мониторинга маршрутизаторов, и коммутаторов, и другой проводной сетевой инфраструктуры. Централизованный сервер управления сетью может быть использован для заливки как конфигурационных настроек, так и обновлений прошивки [firmware] на сетевые устройства.

**Плоскость Контроля [Control Plane]** *Плоскость контроля [control plane]* состоит из контрольной сигнальной информации, и часто определяется как сетевой интеллект или сетевые протоколы. Протоколы динамической маршрутизации 3 уровня, такие как OSPF и BGP, используемые для пересылки данных, являются примером интеллекта плоскости контроля, находящейся в маршрутизаторах. Таблицы памяти с адресацией по содержимому [Content addressable memory (CAM)] и Протокол Ветвящегося Дерева [Spanning Tree Protocol (STP)] являются механизмами плоскости контроля, используемой коммутаторами 2 уровня для пересылки данных.

**Плоскость Данных [Data Plane]** *Плоскость данных [data plane]*, также называемой пользовательской плоскостью [user plane], это местоположение в сети, куда действительно пересыпается пользовательский трафик. Отдельный маршрутизатор, куда пересыпаются IP пакеты, является примером плоскости данных. Отдельный коммутатор, пересылающий кадры 802.3 Ethernet, является примером плоскости данных.

В среде 802.11, эти три логические плоскости работы работают по-разному, в зависимости от типа архитектуры БЛВС и производителя БЛВС. Например, в среде устаревшей автономной ТД, все три плоскости существуют в каждой отдельной точке доступа (хотя, механизмы плоскости контроля минимальны). Когда решения контроллеров БЛВС было впервые представлено в 2002 году, все три плоскости работы были перемещены в централизованное устройство. В современных установках, плоскости работы могут быть разделены между точками доступа, контроллерами БЛВС, и/или беспроводными сетевыми системами управления [wireless network management system (WNMS)].



Не перепутайте плоскости управления, контроля и данных с типами MAC кадров 802.11. В этой главе, обсуждение плоскостей управления, контроля и данных относится к работе сети БЛВС с точки зрения архитектуры.

## Плоскость Управления

Функции *плоскости управления* [*management plane*] в БЛВС 802.11 следующие:

**Конфигурация БЛВС [WLAN Configuration]** Примеры включают конфигурацию настроек SSID, безопасности, WMM, канала, и питания.

**Мониторинг БЛВС и Отчетность [WLAN Monitoring and Reporting]** Статистика мониторинга 2 уровня, такой как ACKs, ассоциации клиентов, переассоциация, скорости передачи данных, происходящая в плоскости управления. Примеры мониторинга верхнего уровня и отчетности включают видимость приложений, IP соединений, пропускной способности TCP, статистику задержки, и сессии межсетевого экрана с отслеживанием состояний соединений [stateful firewall sessions].

**Управление прошивками БЛВС [WLAN Firmware Management]** Это включает способность модернизировать точки доступа и другие устройства БЛВС последним рабочим кодом от производителя. Проще говоря - установкой самого свежего стабильного программного обеспечения на оборудование.

## Плоскость Контроля

*Плоскость контроля* [*control plane*] часто определяется протоклами, которые обеспечивают интеллект и взаимодействие между оборудованием в сети. Вот несколько примеров интеллекта плоскости контроля:

**Адаптивное радио [Adaptive RF]** Настройки согласованного канала и мощности для нескольких точек доступа обеспечиваются плоскостью контроля. Основная часть производителей БЛВС встраивает некий тип функционала адаптивного радио [*adaptive RF*]. Адаптивное радио [Adaptive RF] также называется более техническим термином *управление радио ресурсом* [*radio resource management (RRM)*].

**Механизмы Роуминга [Roaming Mechanisms]** Плоскость управления также обеспечивает поддержку роумингового переключения [handoff] между точками доступа. Функционал может включать роуминг 3его уровня, поддержку клиентских сессий межсетевого экрана с контролем состояний, и отправку забуферизированных пакетов. Механизмы быстрого безопасного роуминга, такие как кэширование гибких ключей [opportunistic key caching (OKC)] и быстрый переход BSS [fast BSS transition (FT)], могут также быть использованы для пересылки мастер-ключей шифрования между точками доступа.

**Балансировка Клиентской Нагрузки [Client Load Balancing]** Сбор и распределение параметров клиентской загрузки и производительности между точками доступа для улучшения общей работы БЛВС происходит в плоскости контроля.

**Протоколы взаимосвязности [Mesh Protocols]** Маршрутизация пользовательских данных между несколькими точками доступа требует некоторого рода протокола взаимосвязной маршрутизации [mesh routing protocol]. Большинство производителей БЛВС используют методы маршрутизации 2ого уровня для перемещения пользовательских данных между взаимосвязанными точками доступа [mesh access points]. Однако, некоторые производители используют взаимосвязную маршрутизацию 3его уровня [layer 3 mesh routing]. Поправка 802.11s определила стандартизованные механизмы взаимосвязной маршрутизации [mesh routing], но производители БЛВС на текущий момент используют собственные (проприетарные) методы и метрики.

## Плоскость Данных

*Плоскость данных [data plane]* - это где пересыпаются пользовательские данные. Два устройства, которые обычно участвуют в плоскости данных - это ТД и контроллер БЛВС. Отдельно стоящая ТД обрабатывает все операции по пересылке данных локально. В решениях с БЛВС контроллером, данные обычно пересыпаются из центрального контроллера, но данные могут также быть отправлены с границы сети точкой доступа. Также как с плоскостями управления и контроля, у каждого производителя есть уникальный способ и рекомендации по управлению пересылкой данных. Модели пересылки данных будут обсуждаться более детально позже в этой главе.

## Архитектура БЛВС

В то время как принятие технологий 802.11 на предприятиях продолжает расти, имеет место быть эволюция архитектуры БЛВС. В большинстве случаев, основная цель технологий 802.11 - это обеспечить беспроводной портал в проводную инфраструктурную сеть. То, как беспроводной портал 802.11 интегрируется в типовую 802.3 Ethernet инфраструктуру, продолжает радикально изменяться. Производители БЛВС в общем предлагают одну из следующих трех первичных архитектур БЛВС:

- Архитектура автономной БЛВС [Autonomous WLAN architecture]
- Архитектура централизованной БЛВС [Centralized WLAN architecture]

- Архитектура распределенной БЛВС [Distributed WLAN architecture]

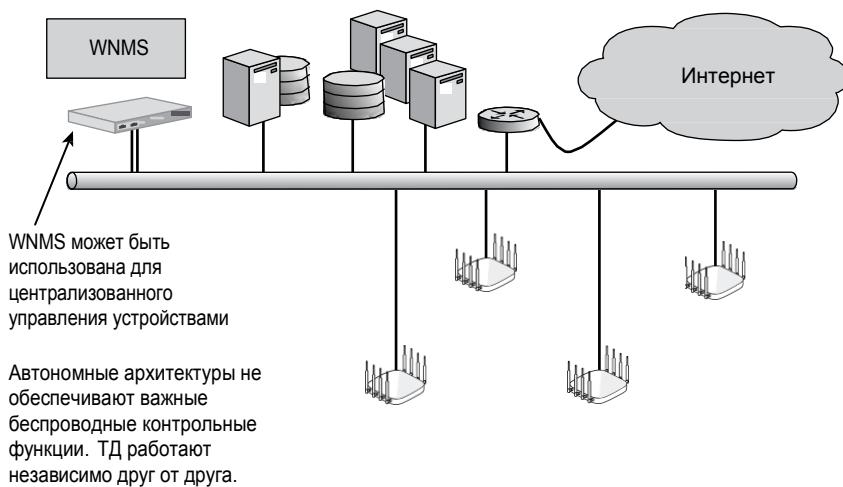
Следующие разделы описывают эти три архитектуры более детально.

## Архитектура Автономной БЛВС

Многие годы, обычные точки доступа были отдельно стоящими устройствами - БЛВС порталами, где присутствовали все три рабочие плоскости, и работали на границе сетевой архитектуры. Эти ТД часто называются как *толстые ТД* [*fat APs*] или *отдельностоящие ТД* [*standalone APs*]. Однако, наиболее распространенный термин в отрасли для традиционной точки доступа - это *автономная ТД* [*autonomous AP*].

Все конфигурационные настройки присутствуют в самой автономной точке доступа, и следовательно, плоскость управления располагается индивидуально в каждой автономной ТД. Все механизмы шифрования и дешифрования и механизмы MAC уровня также работают внутри автономной ТД. Плоскость данных также располагается в каждой автономной ТД, потому что весь пользовательский трафик пересыпается локально каждой индивидуальной точкой доступа. Как показано на Рисунке 11.9, у устаревших автономных ТД есть общие механизмы плоскости контроля.

**РИСУНОК 11.9** Архитектура автономной БЛВС



Автономные точки доступа содержат, как минимум, два физических интерфейса: обычно радиомодуль и порт 10/100/1000 Ethernet. Большую часть времени эти физические интерфейсы связаны вместе в мост [bridged] с виртуальным интерфейсом, который называется виртуальный интерфейс моста [*bridged virtual interface (BVI)*]. Виртуальному интерфейсу моста (BVI) присваивается IP адрес, который является общим для двух и более физических интерфейсов. Точки доступа работают в качестве устройств 2ого уровня; однако, им все-равно нужен адрес 3его уровня для связи с IP сетью. BVI - это интерфейс управления ТД.

Автономная точка доступа содержит стек протокола 802.11, и стек протокола 802.3. Такие ТД могут поддерживать следующие характеристики:

- Несколько интерфейсов управления, таких как команда строка, графический интерфейс web GUI, и SNMP

- Функционалы безопасности WEP, WPA, и WPA2
- Поддержка качества сервиса WMM (WMM quality-of-service)
- Съемные и не съемные антенны
- Возможности фильтрации, такие как фильтрация по MAC и по протоколу
- Режимы связи, такие как доступ(access), взаимосвязность(mesh), мост(bridge), или сенсор(sensor).
- Несколько радиомодулей и двух частотные возможности
- Поддержка 802.1Q VLAN
- Поддержка PoE 802.3af или 802.3at

У автономных ТД могут быть некоторые из следующих улучшенных характеристик безопасности:

- Встроенный RADIUS и базы данных пользователей
- Поддержка VPN клиента и/или сервера
- DHCP сервер
- Перехватывающие веб порталы [Captive web portals]

Автономные ТД устанавливаются на уровне доступа, и обычно запитываются от коммутаторов уровня доступа с поддержкой Power-over-Ethernet (PoE).

Интеграционный сервис в автономной точке доступа транслирует трафик 802.11 в трафик 802.3. Автономная точка доступа была основой, которую архитекторы БЛВС использовали в течение многих лет. Однако, установка автономных точек на предприятиях была заменена на централизованную архитектуру, использующую контроллер БЛВС, которая обсуждается позже в этой главе.

## Централизованная Сетевая Система Управления

Один из вызовов для администратора БЛВС, использующего огромную автономную БЛВС архитектуру, - это управление. Как администратор, захотели бы Вы настроить 300 автономных ТД по отдельности? Главный недостаток использования традиционных автономных точек доступа в том, что нет центральной точки управления. Любая интеллектуальная пограничная БЛВС архитектура с 25 и более автономными точками доступа будет требовать своего рода *систему управления беспроводной сетью [wireless network management system (WNMS)]*.

WNMS убирает плоскость управления [management plane] из автономных точек доступа. WNMS обеспечивает центральную точку управления для настройки и поддержки тысяч автономных точек доступа. WNMS может быть аппаратным комплексом или программным решением. Решения WNMS могут быть под определенного производителя [vendor specific] или под любого производителя [ vendor neutral].

Как ранее показано на Рисунке 11.9, весь смысл сервера WNMS был в обеспечении центральной точки управления для автономных точек доступа, которые теперь считаются устаревшими устройствами. Это определение с годами значительно изменилось. Позже, в этой главе, вы узнаете о контроллерах БЛВС, которые используются в качестве центральных точек управления для ТД, управляемых контроллерами. Контроллеры БЛВС могут фактически заменить WNMS сервер, в качестве центральной точки управления точками доступа, в установках БЛВС небольшого масштаба. Однако, понадобится несколько контроллеров БЛВС в крупномасштабных установках БЛВС уровня предприятия. На текущий момент, большинство серверов WNMS используются сейчас в качестве центральной точки управления для нескольких контроллеров БЛВС в крупномасштабных установках БЛВС уровня предприятия. Сервера WNMS, которые используются для управления несколькими контроллерами БЛВС от одного производителя, могут в некоторых случаях также быть использованы для управления инфраструктурой БЛВС других производителей, включая отдельно стоящие точки доступа.

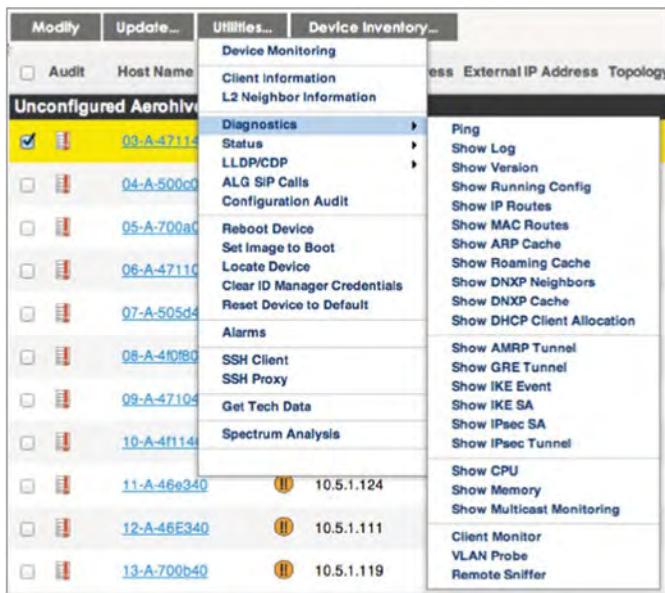
Термин WNMS уже устарел, потому что многие из решений централизованного управления могут также быть использованы для управления другими типами сетевых устройств, включая коммутаторы, маршрутизаторы, межсетевые экраны, и шлюзы VPN. Следовательно, *система управления сетью [network management system (NMS)]* теперь используется более часто. Решения NMS обычно предназначены для определенного производителя [vendor specific]; однако, есть несколько решений, которые могут управлять устройствами от разных производителей сетевых решений.

Эволюция сетевого управления продолжается и большинство современных решений NMS являются облачными. Первые поколения решений NMS базировались на серверах (и на аппаратных комплексах

и на программных решениях). Однако, основная часть решений NMS теперь размещается на облачных платформах. Мы обсудим облачные сети и управление позже в этой главе.

Главная цель NMS – обеспечить центральную точку управления и мониторинга сетевых устройств. Конфигурационные настройки и обновление программного обеспечения (прошивки) могут быть отправлены на все сетевые устройства. Хотя централизованное управление является основной целью, NMS может обладать также и другими возможностями, такими как планирование и управление радиоспектром БЛВС. NMS может также быть использован для мониторинга сетевой архитектуры централизованными аварийными сигналами и оповещениями, и интегрированными в консоль управления. NMS обеспечивает мощный мониторинг сетевой инфраструктуры так же как мониторинг проводных и беспроводных клиентов, подключенных к сети. Как показано на Рисунке 11.10, в решениях NMS обычно присутствуют расширенные диагностические утилиты, которые могут быть использованы для удаленного поиска и устранения проблем (troubleshooting).

**РИСУНОК 11.10** Диагностические утилиты NMS



NMS - это решение плоскости управления; следовательно, ни механизмы плоскости контроля, ни механизмы плоскости данных не присутствуют в NMS. Например, единственная связь между NMS и точкой доступа - это протоколы управления. Большинство решений NMS используют *Простой Протокол Сетевого Управления [Simple Network Management Protocol (SNMP)]* для управления и мониторинга БЛВС. Другие решения NMS также используют протокол *Контроля и Обеспечения Беспроводных Точек Доступа [Control and Provisioning of Wireless Access Points (CAPWAP)]* строго в качестве протокола мониторинга и управления. CAPWAP включает Безопасность Датаграм Транспортного Уровня [*Datagram Transport Layer Security (DTLS)*], чтобы обеспечить шифрование и конфиденциальность данных отслеживаемого трафика управления. Другие безопасные протоколы, такие как HTTPS могут быть использованы для транспортировки

трафика управления от сетевых устройств до сервера NMS или облачной платформы. Пользовательский трафик никогда не пересыпается точкой доступа на NMS; но ассоциации клиентов 802.11 и трафик может мониториться. Рисунок 11.11 показывает экран NMS нескольких клиентских ассоциаций на нескольких ТД.

**РИСУНОК 11.11** Мониторинг клиентов в NMS

REAL TIME	HISTORICAL	8 Connected Clients. Last Updated at 2020-08-30 14:50:09										
STATUS	CONNECTION HEALTH TYPE	HOST NAME	MAC	IPV4	AUTHENTICATION METHOD	USER NAME	OS TYPE	VLAN	SID	DEVICE	CHANNEL	
● WIRELESS	little-chrom...	A402B9BBCB22	10.11.13.100	WPA2-B021X	00:00	CrOS	101	Fadison_E5_Student	E5-AP2	36		
● WIRELESS	mryhaleen-su...	6045BDBEAD4C4	10.11.13.100	WPA2-B021X	mryhaleen	Windows...	103	Fadison_E5_Staff	E5-AP3	151		
● WIRELESS	yury-ipad...	6C19C0CC2A33	10.11.11.102	WPA2-B021X	yurikovs	Apple iOS	101	Fadison_H5_Student	H5-AP2	161		
● WIRELESS	mike-chrom...	A402B9BB4A32	10.11.11.101	WPA2-B021X	mikel...	CrOS	101	Fadison_H5_Student	H5-AP2	161		
● WIRELESS	marcy-chro...	A402B9C34FDD	10.11.12.100	WPA2-B021X	marcy...	CrOS	102	Fadison_MS_Student	MS-AP1	44		
● WIRELESS	vann-surface...	6045BDB6AAF1	10.11.12.100	WPA2-B021X	vanntereb	Windows...	102	Fadison_MS_Staff	MS-AP1	44		
● WIRELESS	cassidy-ipad...	6C19C04D44CD	10.11.12.104	WPA2-B021X	cassidie	Apple iOS	102	Fadison_MS_Student	MS-AP1	44		
● WIRELESS	doreen-chro...	A402B9B23EEE	10.11.12.101	WPA2-B021X	dorenes	CrOS	102	Fadison_MS_Student	MS-AP2	165		

Решения NMS могут быть развернуты в центре обработки данных [data center] компании в виде аппаратного комплекса или виртуального комплекса, который работает на VMware или другой платформе виртуализации. Сервер управления сетью (NMS), который располагается в собственном центре обработки данных компании, часто называется *on-premises NMS* [*дословный перевод: NMS на своих площадях/владениях*]. Как ранее упоминалось, решения NMS также доступны в облаке в виде услуги программного обеспечения по подписке [software subscription service]. Многие производители БЛВС сейчас предлагают доступ к своим решениям NMS по API. Прикладной Программируемый Интерфейс [application programming interface (API)] - это набор подпрограммных определений, протоколов, и инструментов для построения программного обеспечения. Заказчики и партнеры могут использовать API производителя БЛВС, чтобы построить свое собственное пользовательское приложение для мониторинга БЛВС. Собственные приложения заказчиков также могут быть построены для конфигурирования устройств БЛВС. API будет обсуждаться более детально позже в этой главе.

## Архитектура Централизованной БЛВС

Следующий шаг в развитии интеграции БЛВС - это централизованная БЛВС архитектура. Эта модель использует центральный контроллер БЛВС, который располагается в ядре сети. В централизованной архитектуре БЛВС автономные ТД были заменены на точки доступа, управляемые контроллером [*controller-based access points*], также называемые *легковесные ТД* [*lightweight APs*] или *тонкие ТД* [*thin APs*]. Начиная с 2002 года, многие производители БЛВС решили перейти на модель с контроллером БЛВС, где все три логические плоскости работы располагаются внутри контроллера. В централизованной архитектуре БЛВС, три логические плоскости находятся в контроллере БЛВС:

**Плоскость Управления [Management Plane]** Точки доступа настраиваются и управляются с контроллера БЛВС.

**Плоскость Контроля [Control Plane]** Адаптивное радио [Adaptive RF], балансировка нагрузки [load balancing], переключение с ТД на ТД при роуминге [roaming handoffs], и другие механизмы находятся в контроллере БЛВС.

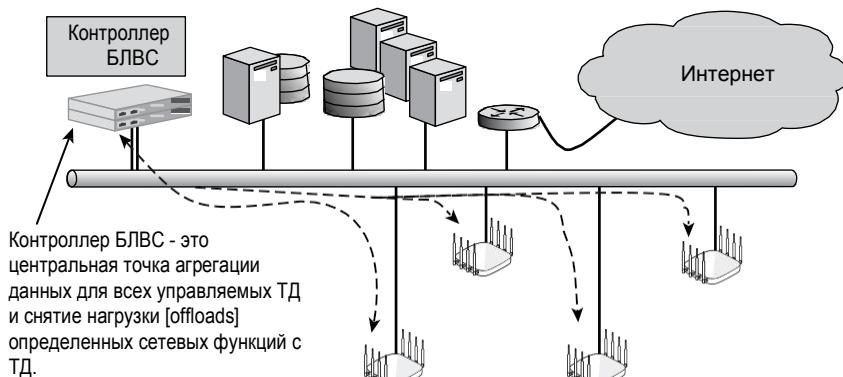
**Плоскость Данных [Data Plane]** Контроллер БЛВС существует в виде точки распределения данных для пользовательского трафика. Точки доступа туннелируют весь пользовательский трафик в центральный контроллер.

Функции шифрования и дешифрования могут находиться в централизованном контроллере БЛВС или могут продолжать поддерживаться ТД, управляемыми контроллером, в зависимости от производителя. Сервис системы распространения [distribution system service (DSS)] и интеграционный сервис [integration service (IS)] обычно оба работают в контроллере БЛВС. Некоторые чувствительные ко времени операции все еще выполняются ТД.

## Контроллер БЛВС

В сердце централизованной архитектуры БЛВС – *контроллер БЛВС [WLAN controller]* (см. Рисунок 11.12). Контроллеры БЛВС иногда назывались как *беспроводные коммутаторы [wireless switches]*, потому что они действительно управляемые Ethernet коммутаторы, которые могут обрабатывать и маршрутизировать данные на Канальном уровне (2 уровне) [Data-Link layer (layer 2)] модели OSI. Многие из контроллеров БЛВС являются многоуровневыми коммутаторами, которые также могут маршрутизировать трафик на Сетевом уровне (3 уровне) [Network layer (layer 3)]. Однако, *беспроводной коммутатор [wireless switch]* стал устаревшим термином и в не достаточной мере описывает многие возможности контроллера БЛВС.

**РИСУНОК 11.12** Архитектура Централизованной БЛВС: контроллер БЛВС



Контроллер БЛВС может предложить многие из следующих возможностей и характеристик:

**Управление ТД [AP Management]** Как упоминалось ранее, большая часть функций точки доступа, таких как мощность, каналы, и поддерживаемые скорости передачи данных настраиваются на контроллере БЛВС. Это позволяет централизованно управлять и настраивать ТД. Некоторые производители используют собственные (проприетарные) протоколы для связи между контроллером БЛВС и его ТД, управляемых контроллером. Эти собственные протоколы могут передавать конфигурационные настройки, обновление ПО, и управлять опросным трафиком [keep-alive traffic]. Протокол

управления БЛВС достигло принятия (признания). Многие производители БЛВС используют протокол *Контроля и Обеспечения Беспроводных Точек Доступа* [*Control and Provisioning of Wireless Access Points (CAPWAP)*] для управления и мониторинга точек доступа. CAPWAP может также быть использован для туннелирования пользовательского трафика между ТД и контроллером БЛВС.

**Управление БЛВС [WLAN Management]** Контроллеры БЛВС способны поддерживать несколько БЛВС, которые часто называются *профилями БЛВС* [*WLAN profiles*] или *профилями SSID* [*SSID profiles*]. Разные группы клиентов 802.11 могут подключаться к разным SSID, который является уникальным для каждого профиля. Профиль БЛВС [*WLAN profile*] – это набор конфигурационных параметров, которые настроены на контроллере БЛВС. Параметры профиля могут включать логическое имя БЛВС (SSID), настройки безопасности БЛВС, назначение VLAN, параметры качества сервиса (QoS). Профили БЛВС часто работают вместе с механизмами контроля доступа на основе ролей [*role-based access control (RBAC)*]. Когда пользователи подключаются к БЛВС, им всегда назначаются определенные роли или пользовательские профили.

**Управление Пользователями [User Management]** Контроллеры БЛВС обычно обеспечивают возможность контролировать кто, когда и где с точки зрения использования механизмов управления доступом на основе ролей [*role-based access control (RBAC)*].

**Мониторинг Устройств [Device Monitoring]** Контроллеры БЛВС обеспечивают визуальный мониторинг ТД и статистику клиентских устройств с точки зрения подключения, роуминга, времени работы и т.д..

**VLANs** Контроллеры БЛВС полностью поддерживают создание VLANов и добавления меток [*tagging*] 802.1Q VLAN. На контроллере БЛВС может быть создано несколько беспроводных пользовательских VLANов, так что пользовательский трафик может быть сегментирован. VLANы могут назначаться статически профилям БЛВС или могут назначаться, используя RADIUS атрибуты. Пользовательские VLANы обычно инкапсулируются в IP туннель.

**Поддержка Безопасности 2 Уровня [Layer 2 Security Support]** Контроллеры БЛВС полностью поддерживают шифрование 2 уровня WEP, WPA и WPA2. Возможности аутентификации включают как внутреннюю базу данных, так и полную интеграцию с RADIUS и LDAP серверами.

**VPN Концентраторы Уровней 3 и 7 [Layer 3 and 7 VPN Concentrators]** Некоторые производители контроллеров БЛВС часто также предлагают возможности VPN сервера внутри контроллера. Контроллер может действовать как VPN концентратор или конечная точка для IPSEC или SSL VPN туннелей.

**Перехватывающий Портал [Captive Portal]** У контроллеров БЛВС есть функционал перехватывающего портала [*captive portal*], который может быть использован в гостевых БЛВС.

**Внутренние Системы Обнаружения Беспроводного Вторжения [Internal Wireless Intrusion Detection Systems]** У некоторых контроллеров БЛВС есть встроенные возможности WIPS для мониторинга безопасности и защиты от неконтролируемых точек доступа [*rogue AP*].

**Возможности Межсетевого Экрана [Firewall Capabilities]** В некоторых БЛВС

контроллерах доступна проверка пакетов с отслеживанием состояний [stateful packet inspection] на внутреннем межсетевом экране.

#### **Автоматическое Восстановление и Балансировка Нагрузки [Automatic Failover and Load Balancing]**

Контроллеры БЛВС обычно обеспечивают поддержку Протокола Резервирования типа Виртуальный Маршрутизатор [Virtual Router Redundancy Protocol (VRRP)] в целях резервирования. Большинство производителей также предлагают собственные (проприетарные) возможности по балансировке нагрузки беспроводных клиентов между несколькими ТД, управляемыми контроллерами. [controller-based APs].

**Управление Адаптивным Радио [Adaptive RF Management]** В большей части контроллеров БЛВС внедрена своего рода функционал *адаптивного радио* [*adaptive RF*]. Контроллер БЛВС – это центральное устройство, которое может динамически изменять конфигурацию управляемых контроллером точек доступа на основе накопленной информации о радиоэфире, собранной с радиомодулей точек доступа. В среде с контроллером БЛВС точки доступа будут мониторить как свои собственные каналы, так и использовать внеканальное сканирование [*off-channel scanning capabilities*] для мониторинга других частот. Любая радиочастотная информация, услышанная любой точкой доступа, сообщается контроллеру БЛВС. На основе всего радиомониторинга [*RF monitoring*] с нескольких точек доступа, контроллер БЛВС производит динамические изменения радиочастотных настроек ТД. Некоторым точкам доступа может быть сказано перейти на другой канал, в то время как другим ТД может быть сказано изменить их настройки мощности передачи.

Адаптивное радио [*Adaptive RF*] иногда называется *управление радио ресурсом* [*radio resource management (RRM)*], и считается интеллектом плоскости управления. Все производители БЛВС применяют свою собственную проприетарную функциональность адаптивного радио. Когда она внедрена, адаптивное радио обеспечивает автоматическую настройку размера соты [*automatic cell sizing*], автоматический мониторинг [*automatic monitoring*], поиск и устранение проблем [*troubleshooting*], и оптимизацию радио среды.

#### **Управление Полосой [Bandwidth Management]**

Ширина полос каналов может быть ограничена по восходящему потоку [*upstream*] или по нисходящему потоку [*downstream*].

#### **Поддержка Роуминга 3 Уровня [Layer 3 Roaming Support]**

Полностью поддерживаются возможности, позволяющие осуществлять бесшовный роуминг через маршрутизируемые границы уровня 3. Более детальное обсуждение роуминга 3 уровня и стандарта Мобильного IP можно найти в Главе 13..

#### **Питание по Ethernet [Power over Ethernet (PoE)]**

При развертывании на уровне доступа, контроллеры БЛВС могут напрямую подать питание на управляемые контроллером точки доступа по PoE. Однако, большинство ТД, управляемых контроллером, запитываются сторонними пограничными коммутаторами.

#### **Интерфейсы Управления [Management Interfaces]**

Многие контроллеры БЛВС предлагают полную поддержку общепринятых интерфейсов управления таких, как GUI(графический интерфейс), CLI (интерфейс командной строки), SSH, и т.д.

Контроллеры БЛВС могут поставляться во множестве форм факторов и размерах. Традиционный контроллер БЛВС - это аппаратный комплекс. Производители Wi-Fi также предлагают контроллеры БЛВС в виде программного обеспечения, которое работает в виртуализированной среде такой, как VMware. Также некоторые производители предлагают контроллеры БЛВС в виде аппаратных или программных модулей, которые могут быть интегрированы в проводной коммутатор. Контроллеры для крупных предприятий могут быть способны управлять и терминировать трафик с 1000 ТД. Младшая модель контроллеров БЛВС может управлять 25 точками доступа.

## Разделение функций контроля доступа к среде [Split MAC]

Большая часть производителей контроллеров БЛВС внедрила, что называется *архитектурой с разделением функций контроля доступа к среде [split MAC architecture]*. С этим типом архитектуры БЛВС, некоторые сервисы контроля доступа к среде (MAC service) выполняются контроллером БЛВС, а некоторые выполняются точкой доступа. Например, интеграционный сервис и сервис системы распространения осуществляется контроллером. Методы WMM QoS обычно выполняются контроллером. В зависимости от производителя, шифрование и дешифровка кадров данных 802.11 может выполняться контроллером или ТД.

Вы уже знаете, что кадры 802.11 туннелируются между ТД, управляемыми только контроллером, и контроллером БЛВС. Кадры данных 802.11 обычно туннелируются до контроллера, потому что интеграционный сервис контроллера переносит полезную нагрузку MSDU уровней 3-7 кадров данных 802.11 в кадры 802.3, которые отправляются в сетевые ресурсы. Фактически, контроллеру БЛВС нужно обеспечить централизованный шлюз к сетевым ресурсам для полезной нагрузки кадров данных 802.11. У кадров 802.11 управления и контроля нет полезной нагрузки верхних уровней, и, следовательно, они никогда не транслируются в кадры 802.3. Кадрам 802.11 управления и контроля нет необходимости быть туннелированными до контроллера БЛВС, потому что контроллер не должен обеспечивать шлюз к сетевым ресурсам для этих типов кадров 802.11.

В архитектуре с разделением функций контроля доступа к среде [split MAC architecture], большой обмен кадрами 802.11 управления и контроля происходит только между клиентской станцией и ТД, управляемой только контроллером, а не туннелируются до контроллера БЛВС. Например, маяки [beacons], зондирующие ответы [probe responses], и подтверждения [ACKs] могут быть сгенерированы ТД, управляемой только контроллером, вместо самого контроллера. Стоит отметить, что большинство решений контроллеров БЛВС применяют архитектуру с разделением функций MAC [split MAC architectures] по-разному. Много решений контроллеров БЛВС используют протокол *Контроля и Обеспечения Беспроводных Точек Доступа [Control and Provisioning of Wireless Access Points (CAPWAP)]* для мониторинга и управления. CAPWAP также определяет функционал разделения функций контроля доступа к среде (MAC). Протокол CAPWAP может быть использован, чтобы туннелировать трафик 802.11 между ТД и контроллером БЛВС.



Подробную информацию о протоколе Контроля и Обеспечения Беспроводных Точек Доступа [Control and Provisioning of Wireless Access Points (CAPWAP)] можно найти на веб сайте IETF, в RFC 5415, <https://tools.ietf.org/html/rfc5415>.

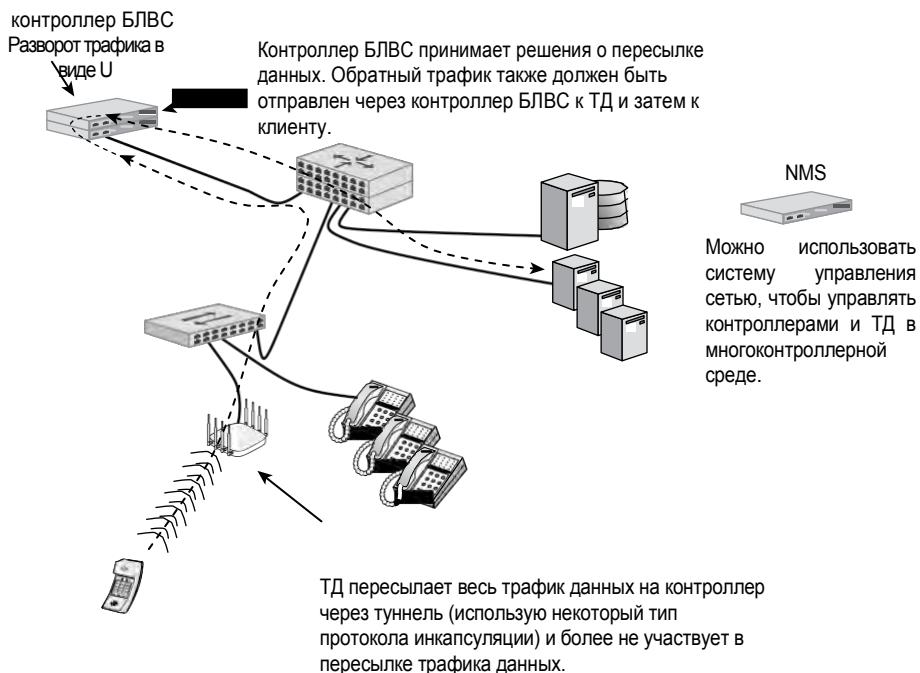
## Модели Пересылки Данных Контроллером

Ключевая характеристика большинства контроллеров БЛВС в том, что интеграционный сервис (IS) и сервисы (службы) системы распространения (DSS) работают в контроллерах БЛВС. Другими словами, весь пользовательский трафик 802.11, который направлен в проводную сторону сетевых ресурсов, должен сначала пройти через контроллер, и быть транслирован в трафик 802.3 интеграционным сервисом, прежде чем быть отправленным к финальному проводному месту назначения. Следовательно, точки доступа, управляемые только контроллером, отправляют свои кадры 802.11 к контроллеру БЛВС по проводному 802.3 соединению.

Формат кадра 802.11 сложный и разработан для беспроводной среды, не проводной среды. Кадр 802.11 не может пройти через сеть 802.3 Ethernet сам. Так, как кадр 802.11 может перемещаться между ТД, управляемой только контроллером, и контроллером БЛВС? Трафик 802.11 пересыпается внутри инкапсулированного в IP туннеля. Каждый кадр 802.11 целиком инкапсулируется в тело IP пакета. Многие производители БЛВС используют Универсальную Маршрутизируемую Инкапсуляцию [*Generic Routing Encapsulation (GRE)*], которая является общепринятым используемым сетевым протоколом туннелирования. Хотя GRE часто используется для инкапсуляции IP пакетов, GRE также может быть использован для инкапсуляции кадра 802.11 внутрь IP туннеля. GRE туннель создает виртуальный канал точка-точка между ТД, управляемой только контроллером, и самим контроллером БЛВС. Хотя GRE – это наиболее типовой выбор, производители БЛВС могут использовать IPSec или собственные проприетарные протоколы для IP туннелирования. Протокол управления CAPWAP также может быть использован для туннелирования пользовательского трафика.

Как показано на Рисунке 11.13, ТД, управляемая только контроллером, туннелирует все свои кадры 802.11 обратно к контроллеру БЛВС, с уровня доступа и до уровня ядра. Служба системы распространения внутри контроллера направляет трафик, в то время как интеграционный сервис преобразует данные MSDU 802.11 в кадр 802.3. После того как кадры данных 802.11 преобразованы в кадры 802.3, они отправляются к своему конечному проводному пункту назначения.

РИСУНОК 11.13 Централизованная пересылка данных



Большинство контроллеров БЛВС устанавливаются на уровне ядра [core layer]; однако, они могут также быть развернуты и на уровне распределения [distribution layer], или даже на уровне доступа [access layer]. Где точно устанавливается контроллер БЛВС зависит от решения производителя БЛВС и предполагаемой интеграции беспроводной сети в уже существующую проводную топологию. Несколько контроллеров БЛВС, которые взаимодействуют друг с другом, могут быть развернуты на разных сетевых уровнях при условии, что они могут обмениваться данными друг с другом.

Существует два типа способов пересылки данных при использовании контроллеров БЛВС:

**Централизованная Пересылка Данных [Centralized Data Forwarding]** Все данные пересыпаются от ТД к контроллеру БЛВС для обработки. Это может быть использовано во многих случаях, особенно когда контроллер БЛВС управляет шифрованием и дешифровкой, или применяет политики безопасности или качества (QoS).

**Распределенная Пересылка Данных [Distributed Data Forwarding]** ТД выполняет пересылку данных локально. Это может быть использовано в ситуации, где более выгодно выполнять пересылку на границе сети и избегать центральной локации в сети для всех данных, которые могут потребовать значительных ресурсов процессора и памяти у контроллера.

Как показано на Рисунке 11.13, централизованная пересылка данных полагается на контроллер БЛВС для пересылки данных. ТД и контроллер БЛВС формируют инкапсулированный в IP туннель, и весь пользовательский трафик передается на контроллер для пересылки (или приходит из контроллера). По сути, ТД играет пассивную роль в обращении с пользовательскими данными.

Как проиллюстрировано на Рисунке 11.14, в сценарии с распределенной пересылкой, ТД единственная ответственная за определение того как и куда переслать пользовательский

РИСУНОК 11.14 Распределенная пересылка данных



трафик данных. Контроллер не является активным участником в этих процессах. Это включает применение политик качества (QoS) или безопасности к данным. Вообще говоря, устройства, которые выполняют большую часть функции контроля доступа к среде [MAC], также вероятнее всего выполняют пересылку данных [data forwarding]. Решение использовать распределенную или централизованную пересылку основывается на ряде факторов, таких как безопасность, VLANы, и пропускная способность. Основной недостаток распределенной пересылки данных в том, что некоторые механизмы плоскости контроля могут быть недоступны, потому что они существуют только в контроллере БЛВС. Механизмы плоскости контроля, которые могут быть потеряны, включают адаптивное радио [adaptive RF] роуминг 3-го уровня [layer 3 roaming], применение политик межсетевого экрана [firewall policy enforcement], и быстрый безопасный роуминг [fast secure roaming]. Однако, по мере развития контроллерной архитектуры, некоторые производители БЛВС также вернули некоторые механизмы плоскости контроля обратно в ТД на границе сети.

Так как технология 802.11 и полоса [bandwidth] становятся все больше и больше преобладающими в больших сетях предприятий, то централизованная пересылка данных [centralized data forwarding] может стать более сложной и дорогой из-за трафиковой нагрузки, которая теперь может быть создана на БЛВС. Огромные контроллеры с каналами 10Гбит/с стали более распространенными. Кроме того, производители контроллеров БЛВС теперь начинают применять распределенную пересылку данных [distributed data forwarding] разными способами.

## Контроллер БЛВС Удаленного Офиса

Хотя обычно контроллеры БЛВС располагаются в ядре сети, они также могут быть развернуты на уровне доступа, обычно в форме контроллера БЛВС удаленного офиса. У контроллера БЛВС удаленного офиса обычно меньшая мощность обработки, чем у контроллера БЛВС ядра, и он также менее дорогой. Назначение контроллера БЛВС удаленного офиса – позволить удаленному офису и филиалу быть управляемыми из одного места.

Удаленные контроллеры БЛВС обычно связываются с центральным контроллером БЛВС через WAN канал. Обычно на WAN соединении между контроллерами доступен функционал безопасного VPN туннелирования. Через VPN туннель центральный контроллер может загрузить сетевые конфигурационные настройки на удаленный контроллер БЛВС, который затем будет управлять и контролировать локальные ТД. Этим удаленным контроллерам доступно только ограниченное число ТД, управляемых только контроллером. Типовые характеристики включают: Питание по Ethernet [Power over Ethernet], внутренний межсетевой экран, и встроенный маршрутизатор, использующий NAT и DHCP для сегментации.

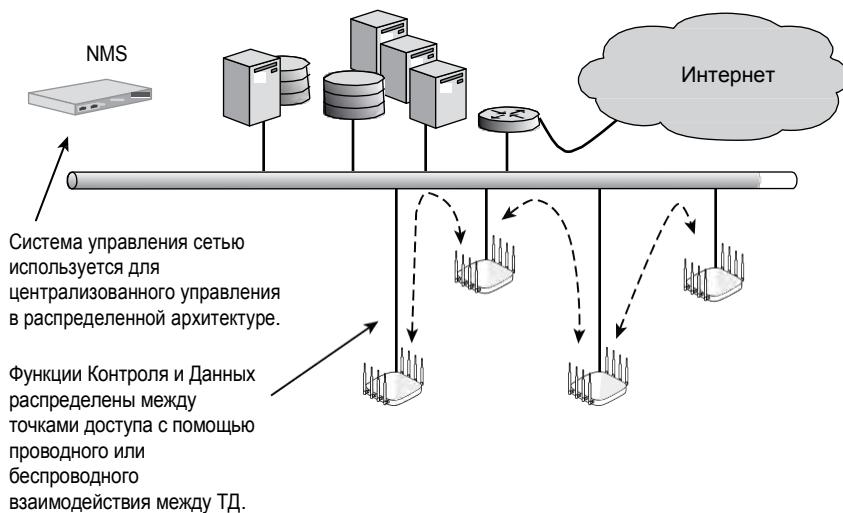
## Распределенная Архитектура БЛВС

Растет тенденция ухода от архитектуры с централизованным контроллером БЛВС к распределенной архитектуре. Некоторые производители БЛВС спроектировали свои системы БЛВС полностью вокруг распределенной архитектуры. Некоторые производители контроллеров БЛВС теперь также предлагают решения по распределенной архитектуре БЛВС, в дополнение к своему решению на основе контроллера. В этих системах используются совместно работающие точки доступа [cooperative access points], и механизмы плоскости контроля работают в системе по взаимодействия между ТД [inter-AP communication] по протоколам совместной работы [cooperative protocols].

Распределенная архитектура БЛВС объединяет несколько точек доступа с набором протоколов совместной работы, не требуя контроллера БЛВС. Распределенные архитектуры БЛВС смоделированы по традиционным моделям проектирования маршрутизации[routing] и коммутации[switching], в том, что сетевые узлы обеспечивают независимый распределенный интеллект, но работают вместе как система, совместно предоставляя механизмы контроля.

Как показано на Рисунке 11.15, протоколы позволяют нескольким ТД организовываться в группы, которые делятся информацией плоскости управления между ТД, чтобы обеспечить функции, такие как роуминг 2 уровня, роуминг 3 уровня,

**РИСУНОК 11.15** Распределенная архитектура БЛВС



применение политик межсетевого экрана, совместное радиочастотное управление, безопасность, и взаимосвязные сети [mesh networking]. Лучший способ описать распределенную архитектуру - это представить группу точек доступа с большей частью интеллекта контроллера БЛВС и возможностями, упомянутыми ранее в этой главе. Информации плоскости контроля делится между ТД, используя проприетарные протоколы.

В распределенной архитектуре, каждая индивидуальная точка доступа ответственна за локальную пересылку пользовательского трафика. Как упоминалось ранее, с приходом 802.11n, производители контроллеров БЛВС стали предлагать решения по распределенной пересылке данных, чтобы управлять нагрузкой трафика. Так как распределенная архитектура БЛВС полностью устраняет централизованный контроллер БЛВС, весь пользовательский трафик пересыпается локально каждой независимой ТД. В распределенной архитектуре плоскость данных находится в точках доступа на границе сети. Никакого контроллера БЛВС нет, следовательно, данным не нужно быть туннелированным в ядро сети.

Хотя плоскость контроля и плоскость данных вернулись обратно в ТД в распределенной архитектуре БЛВС, плоскость управления осталась централизованной. Конфигурация и мониторинг всех точек доступа в распределенной модели все еще управляется решениями систем сетевого управления (NMS). Большинство сегодняшних ТД распределенных архитектур управляется NMS, которая работает как облачный сервис. Однако, производители Wi-Fi обычно предлагают свои решения NMS как устанавливаемый у заказчика сервер [on-premises server]. Большинство функций, упомянутых в предыдущем разделе о контроллерах БЛВС, могут также быть найдены в распределенной архитектуре БЛВС, даже несмотря на то, что там нет контроллера БЛВС. Например, перехватывающий веб портал [captive web portal], который обычно размещается в контроллере БЛВС, располагается в индивидуальных ТД. Межсетевой экран с контролем состояний [stateful firewall] и возможности RBAC, находящиеся в центральном контроллере БЛВС, теперь существуют совместно [cooperative] в точках доступа. Внутренние [Back-end] механизмы роуминга и адаптивного радио также существуют совместно [cooperative]. ТД также могут работать как RADIUS сервер с полными возможностями интеграции с LDAP. Как упоминалось ранее, все механизмы плоскости контроля присутствуют во взаимодействии между точками доступа на границе сети в распределенной архитектуре БЛВС. ТД реализуют механизмы плоскости контроля, совместно используя проприетарные протоколы.

Как организуются VLANы в среде БЛВС зависит от дизайна сети, а также типом архитектуры БЛВС. Очень большая разница в использовании между моделью на основе контроллера и модели без контроллера в том, как реализованы VLANы в сетевом дизайне. В модели с контроллером БЛВС, основной пользовательский трафик централизовано пересыпается на контроллер от ТД. Так как весь пользовательский трафик инкапсулирован, ТД, управляемые только контроллером, обычно подключены к порту доступа [access port] на Ethernet коммутаторе, который связан с единственным VLANом.

В архитектуре с контроллером БЛВС, пользовательские VLANы обычно размещаются в ядре сети. Пользовательские VLANы не доступны на коммутаторе уровня доступа. ТД, управляемые только контроллером, подключены к порту доступа [access port] пограничного коммутатора [edge switch]. Пользовательские VLANы все еще доступны беспроводным пользователям, потому что все пользовательские VLANы инкапсулированы в IP туннель между ТД, управляемой только контроллером, на границе и контроллером БЛВС в ядре.

Модель без контроллера [noncontroller model], однако, требует поддержку нескольких пользовательских VLANов на границе [edge] сети. Каждая точка доступа, следовательно, подключена к транковому 802.1Q порту на пограничном коммутаторе, который

поддерживает метки VLANов [VLAN tagging]. Все пользовательский VLANы настраиваются на коммутаторе уровня доступа. Точки доступа подключены к транковому 802.1Q порту пограничного коммутатора. Метки [tag] пользовательских VLANов добавляются в транк 802.1Q, и весь беспроводной пользовательский трафик пересыпается на границе сети.

Хотя весь смысл модели совместной работы и распределенного БЛВС в том, чтобы избежать центральной пересылки пользовательского трафика в ядре, точки доступа всё же могут иметь способности IP туннелирования. Некоторые заказчики БЛВС требуют, чтобы трафик гостевого VLANa не пересекал внутренние сети. В таком сценарии, отдельно стоящая ТД может пересыпать только трафик гостевого пользовательского VLANa в IP туннеле, который терминируется на другой отдельно стоящей ТД, которая развернута в DMZ. Отдельные ТД могут также работать как VPN клиент или VPN сервер, используя шифрованные IPSec туннели через канал WAN.

Еще одно преимущество распределенной архитектуры БЛВС – это масштабируемость. По мере роста компании в одной локации или нескольких локациях, очевидно нужно будет установить дополнительные ТД. В решениях с контроллером БЛВС, возможно, что нужно будет купить дополнительные контроллеры и развернуть их по мере роста количества ТД. В распределенной архитектуре БЛВС без контроллера, только устанавливаются только новые ТД по мере роста компании. Многие вертикальные рынки, такие как сфера образования от детского сада до последнего класса 12и летней школы [K–12 education] и сфера розничной торговли, имеют школы и магазины в многочисленных локациях. Распределенная архитектура БЛВС может быть лучшим выбором по сравнению с установкой контроллера БЛВС в каждой локации.

## Гибридная Архитектура БЛВС

Важно понимать, что ни одна из архитектур БЛВС, описанных в этой главе, не высечена в камне. Много гибридов этих архитектур БЛВС существует среди производителей БЛВС. Как уже упоминалось, некоторые производители контроллеров БЛВС выносят некоторый интеллект плоскости контроля обратно на точки доступа. У одного производителя [на момент перевода уже многих производителей] контроллеров БЛВС есть облачный контроллер, где большая часть интеллекта находится в облаке.

Обычно плоскость данных централизована при использовании контроллеров БЛВС, но распределенная пересылка данных также доступна. Некоторые производители БЛВС сдвинули плоскость данных обратно на границу сети в ТД, выполняющими пересылку данных пользовательского трафика. В бесконтроллерной распределенной архитектуре БЛВС все данные пересыпаются локально, но возможность централизовать плоскость данных является характеристикой распределенной архитектуры БЛВС. В общем, у большинства производителей БЛВС теперь есть выбор или централизованной или локальной пересылки плоскости данных в зависимости от размещения точек доступа и доступных маршрутов трафика.

В распределенной архитектуре БЛВС, плоскость управления размещается на своих площадях [on-premises] или на облачной сервисе управления сетью. В модели с контроллером БЛВС, плоскость управления обычно находится в контроллере БЛВС. Однако, плоскость управления может быть также перенесена на NMS, которая управляет не только ТД, управляемыми только контроллером, но также и контроллерами БЛВС.

# Специальная Инфраструктура БЛВС

В предыдущих разделах, мы обсуждали развитие устройств сетевой инфраструктуры БЛВС, которая используется для интеграции беспроводной сети 802.11 в проводную сеть архитектуру. Рынок Wi-Fi произвел множество специальных устройств БЛВС в дополнение к ТД и контроллерам БЛВС. Многие из этих устройств, такие как мосты [bridges] и взаимосвязанные сети [mesh networks], стали чрезвычайно популярными, хотя они работают за пределами определенных стандартов 802.11. Вы увидите эти устройства в следующих разделах.

## Филиальные Маршрутизаторы БЛВС Предприятия

В дополнение к главному корпоративному офису, у компаний часто есть филиальные офисы в удаленных локациях. У компаний могут быть офисы филиалов в регионе или по всей стране, или они могут быть распределены по всему миру. Вызов для IT персонала в том, как обеспечить бесшовные проводные и беспроводные решения уровня предприятия по всем локациям. Распространенное решение - использование маршрутизаторов БЛВС уровня предприятия в каждом филиальном офисе, является обычным выбором.

Держите в уме, что филиальные маршрутизаторы БЛВС [WLAN branch routers] очень отличаются от точек доступа. В отличие от точек доступа, которые используют виртуальный интерфейс моста, у беспроводных маршрутизаторов отдельные маршрутизуемые [routed] интерфейсы. Радиокарты находятся в одной подсети, в то время как WAN Ethernet порт в другой подсети.

У филиальных маршрутизаторов филиальной БЛВС есть возможность подключиться к корпоративной штаб-квартире по VPN туннелю. Сотрудники в филиальных офисах могут получать доступ к корпоративным ресурсам через WAN через VPN туннель. Даже более важен тот факт, что корпоративные VLANы, SSID, и безопасность БЛВС могут все быть расширены на удаленные офисы филиалов. Сотрудники филиальных офисов подключаются к тому же самому SSID, к которому подключились бы в корпоративных штаб-квартирах. Политики проводного и беспроводного доступа, следовательно, непрерывны по всей организации. Эти бесшовные политики могут быть расширены на маршрутизаторы БЛВС в каждой филиальной локации.

Филиальные маршрутизаторы БЛВС уровня предприятия очень похожи на маршрутизаторы Wi-Fi потребительского класса, которые большинство из нас используют дома. Однако, маршрутизаторы БЛВС уровня предприятия производятся на оборудовании лучшего качества и предлагают более широкий массив функций.

Следующие функции безопасности часто поддерживаются маршрутизаторами БЛВС уровня предприятия:

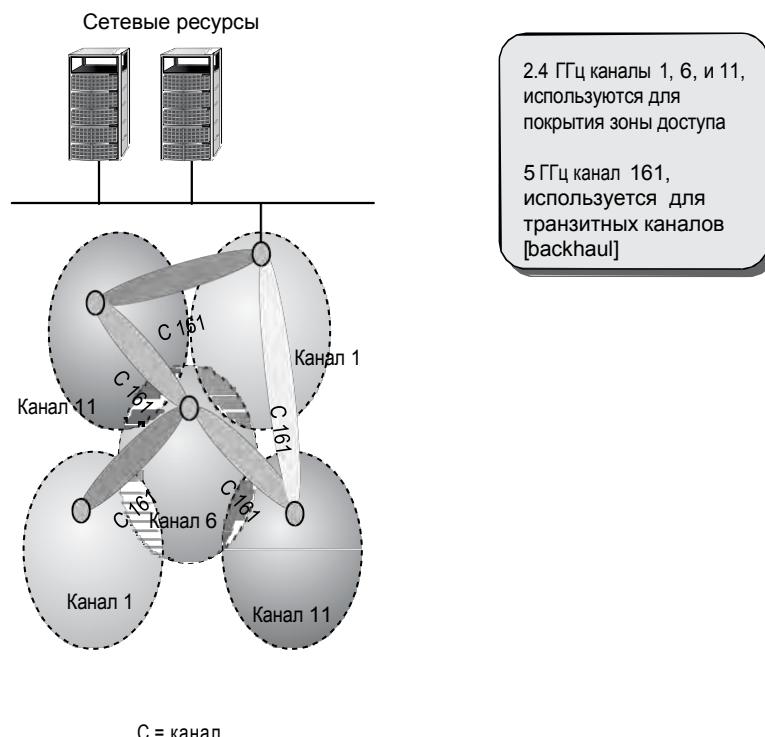
- Безопасность 802.11 2ого уровня для беспроводных клиентов
- Безопасность порта 802.1X/EAP для проводных клиентов
- Сетевая трансляция адресов (Network address translation (NAT))
- Портовая трансляция адресов (Port address translation (PAT))
- Проброс портов (Port forwarding)

- Межсетевой Экран (Firewall)
- Встроенный VPN клиент
- Транзит сотового трафика 3G/4G

## Взаимосвязные Точки Доступа БЛВС

Почти все производители БЛВС сейчас предлагают функционалы *взаимосвязанных точек доступа БЛВС* [*WLAN mesh access point*]. Беспроводные взаимосвязанные (mesh) ТД связываются друг с другом с использованием проприетарных протоколов маршрутизации 2 уровня, и создают само-формирующуюся и самовосстанавливающуюся беспроводную инфраструктуру (взаимосвязь [mesh]), через которую пограничные устройства могут связываться, как показано на Рисунке 11.16. Главное назначение взаимосвязанной БЛВС [mesh WLAN] - это обеспечить беспроводной клиентский доступ в физической области, где Ethernet кабель не может быть подключен к ТД. Клиентский трафик БЛВС может быть отправлен через беспроводной транзитный канал [backhaul] с конечным назначением взаимосвязанными порталами [mesh portals], которые подключены к проводной сети.

**РИСУНОК 11.16** Взаимосвязанная сеть БЛВС(WLAN mesh network)



Взаимосвязанные [mesh] сети БЛВС автоматически подключают точки доступа после инсталляции и динамически обновляют маршруты трафика по мере большего добавления клиентов. Проприетарные интеллектуальные протоколы маршрутизации 2ого уровня определяют динамические маршруты, базируясь на измерениях трафика, силы сигнала, скоростей передачи данных, количестве скачков (hops), и других параметров.

В двух диапазонных беспроводных взаимосвязанных ТД, обычно 5ГГц радиомодули используются для взаимосвязанных транзитных каналов, как показано на Рисунке 11.16. Взаимосвязанный транзитный трафик должен также быть зашифрован. В некоторых случаях 2,4ГГц взаимосвязанный транзитный канал связи может быть использован вместо 5ГГц. В ближайшем будущем, 6 ГГц транзитные каналы [backhaul] связи будут наиболее вероятно общепринятой стратегией по развертыванию взаимосвязности (mesh). В большинстве случаев, безопасность 802.11 с предварительно известным общим ключом [802.11 preshared key (PSK)] используется между взаимосвязанными радиомодулями, чтобы обеспечить шифрование. PSK обычно создается автоматически в большинстве решений взаимосвязанной [mesh] БЛВС. Следует использовать очень сильный пароль из 20 знаков или более, если производитель БЛВС предлагает вариант с ручным определением безопасности взаимосвязанного транзитного канала [mesh backhaul].

## Мосты БЛВС

Общепринятое специфичное развертывание технологии 802.11 - это *беспроводной мост ЛВС* [*wireless LAN bridge*]. Назначение мостов в обеспечении беспроводной связи между двумя и более проводными сетями. Мост в общем поддерживает все те же самые характеристики, которыми обладает автономная точка доступа, но назначение в подключении проводных сетей, а не в обеспечении беспроводной связи для клиентских станций. Когда здания отделены друг от друга и между ними нет никакой сетевой проводной инфраструктуры, то часто применяются беспроводные мосты. Затраты на ежемесячно оплачиваемый телекоммуникационный канал могут быть уменьшены на одноразовые затраты на беспроводной мост точка-точка [*point-to-point (PtP)*]. Беспроводные мосты также используются между башнями/вышками связи и могут иногда распространяться на несколько миль.

Мост и транзитные каналы [backhaul] имеют тенденцию иметь совершенно другие требования, чем обычная ТД, которая обслуживает клиентов БЛВС. Первое различие в том, что ТД обычно работает на уровне доступа [*access layer*] сети. Мосты БЛВС работают на уровне распространения [*distribution layer*], и обычно используются для соединения двух или более проводных сетей вместе по беспроводному каналу связи.

Внешние мостовые каналы связи [*Outdoor bridge links*] используются снаружи, чтобы соединить внутренние проводные сети двух зданий. Внешний мостовой канал связи часто используется как избыточный резервный канал для T1 или волоконно-оптического соединения между зданиями. Внешние мостовые беспроводные каналы связи даже более обычно используются для замены T1 или оптоволоконных соединений между зданиями, из-за их солидной экономии затрат.

Беспроводные мосты поддерживают две главные конфигурационные настройки: *корневой [root]* и *некорневой [nonroot]*. Мосты работают в взаимоотношении родитель/ребенок [*parent/child*], поэтому думайте о корневом мосте [*root bridge*] как о родителе, а некорневом мосте [*nonroot bridge*] как о ребенке.

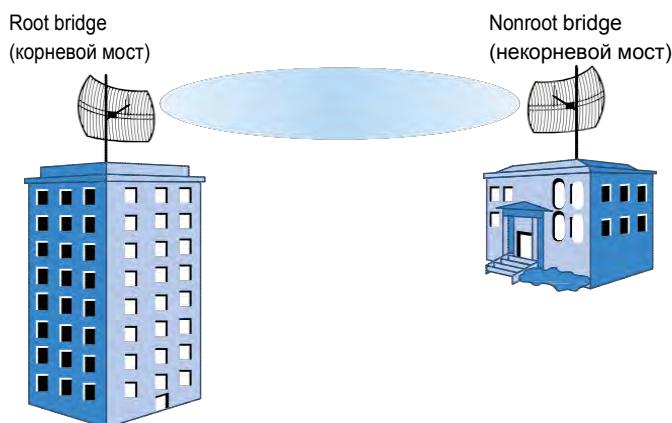
Одна сторона канала обычно корневой мост, а другая – некорневой мост. Корневой мост устанавливает канал и маяки для того, чтобы некорневой мост присоединился. Некорневой мост затем ассоциируется с корневым мостом в похожей манере, как и клиентская станция, чтобы установить канал связи.

Мостовой канал связи, который соединяет только две проводные сети, называется мост *точка-точка [point-to-point (PtP) bridge]*. Рисунок 11.17 показывает соединение PtP между двумя проводными сетями с использованием двух мостов 802.11 и направленных антенн.

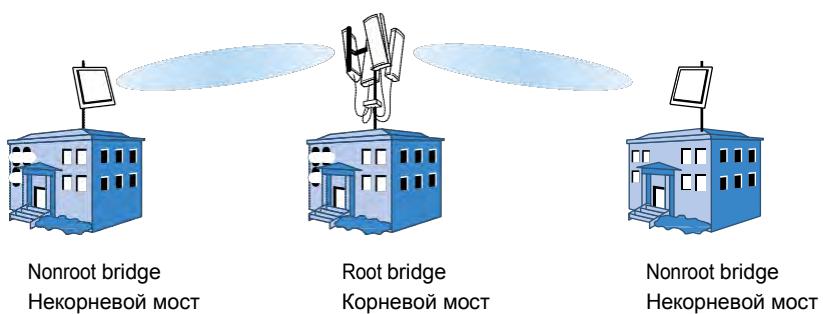
Заметьте, что один из мостов должен быть сконфигурирован в качестве родительского корневого моста, а другой мост сконфигурирован в качестве некорневого моста типа ребенок.

Мостовой канал связи *точка-многоточка* [*point-to-multipoint (PtMP)*] соединяет несколько проводных сетей. Корневой мост является центральным мостом, а несколько некорневых мостов соединяются с корневым мостом. Рисунок 11.18 показывает мостовой канал связи PtMP между тремя зданиями. Пожалуйста, обратите внимание, что корневой мост использует всенаправленный антенный массив с высоким усилением, в то время как все некорневые мосты используют однонаправленные антенны, направленные на антенну корневого моста. Также заметьте, что существует только один корневой мост в соединении PtMP. И никогда не может быть более одного корневого моста.

**РИСУНОК 11.17** Мост БЛВС точка-точка



**РИСУНОК 11.18** Мост БЛВС точка-многоточка



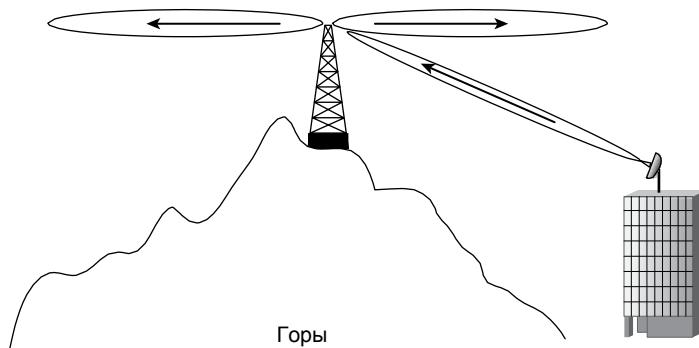
Параметры, принимаемые во внимание, при развертывании наружных каналов-мостов, многочисленны, и включают в себя зону Френеля, выпуклость земли, потери на пути в свободном пространстве, бюджет линии связи, запас на замирание [fade margin]. Могут быть и другие условия, принимаемые во внимание, такие как разрешенные мощности расчетного излучателя [IR] и ЭИИМ [EIRP], в соответствии с определениями регуляторного органа вашей страны.

Каналы связи точки-точка в полосе 2,4ГГц могут простираться на несколько миль. Проблема, которая может случиться на длинном канале связи - это превышение

лимита времени ожидания ACK [ACK timeout]. Из-за полудуплексной природы среды, каждый односторонний [unicast] кадр должен быть подтвержден. Следовательно, односторонний кадр, отправленный по длинному PtP каналу связи одним мостом, должен немедленно получить кадр ACK от противоположного моста, отправленного обратно по тому же самому длинному каналу связи. Не смотря на то что радиоволны перемещаются со скоростью света, ACK может быть получен недостаточно быстро. У исходного моста закончится время, после не получения кадра ACK за определенное количество микросекунд, и он сделает предположение, что произошел конфликт (коллизия). Исходный мост тогда осуществит повторную передачу [retransmit] одностороннего кадра даже несмотря на то, что кадр ACK уже может быть в пути. Повторная передача одностороннего [unicast] трафика, которому не нужно быть отправлено повторно, может привести к деградации пропускной способности до 50 процентов. Чтобы решить эту проблему, у большинства мостов есть настройки времени ожидания ACK [ACK timeout], который может быть подстроен, чтобы разрешить более длительный период времени ожидания для того, чтобы мост получил кадр ACK через длинный канал связи.

Типовая проблема с мостами точка-многоточечка - это установка всенаправленной антенны с высоким уровнем усиления корневого моста слишком высоко, как изображено на Рисунке 11.19. Результатом является то, что вертикальная линия прямой видимости с направленными антеннами некорневых мостов является непригодной. Решением для этой проблемы является использование всенаправленных антенн с высоким уровнем усиления, которые обеспечивают определенного размера электрический наклон, или использование направленных секторных антенн, выровненных для обеспечения всенаправленного покрытия.

**РИСУНОК 11.19** Общая проблема мостов



Для защиты конфиденциальности данных по транзитной связи через мостовые каналы связи нужно шифрование. IPsec VPNs иногда используется для безопасности мостов, которая будет обсуждаться в Главе 17 "802.11 Архитектура Сетевой Безопасности". Решение 802.1X/EAP может также быть использовано для безопасности мостов, где корневой мост предполагается в роли аутентификатора (или подтверждающего) [authenticator role], а некорневые мосты предполагаются в роли клиентов [supplicant role]. Дополнительно, аутентификация PSK часто используется для безопасности мостов БЛВС, и, следовательно, рекомендуется сильный пароль из 20 знаков и более.

## Системы Позиционирования Реального Времени

У решений NMS, контроллеров БЛВС, и решений WIPS есть некоторые встроенные возможности отслеживать перемещение [track] клиентов 802.11, используя точки доступа в качестве датчиков. Однако, возможности по отслеживанию [tracking] являются не обязательно реального времени, и могут быть с точностью только примерно 25 футов (7,62 метра). Возможности отслеживания местоположения [tracking] в контроллерах БЛВС и решениях WIDS предоставляют решение почти реального времени или недавнего времени [near-time] и не могут обслуживать Wi-Fi RFID метки. Несколько компаний, такие как Стэнли Хелскеа [Stanley Healthcare], предоставляют *систему позиционирования реального времени [real-time location system (RTLS)]* БЛВС, которая может отслеживать положение [track the location] любого радиоустройства 802.11, а также метки Wi-Fi RFID с существенно большей точностью. Компоненты вышеперечисленного решения RTLS БЛВС включают предварительно существующую инфраструктуру БЛВС, предварительно существующие клиенты БЛВС, метки Wi-Fi RFID, и сервер RTLS. Дополнительные датчики RTLS БЛВС могут также быть добавлены, чтобы дополнить предварительно существующие ТД БЛВС.

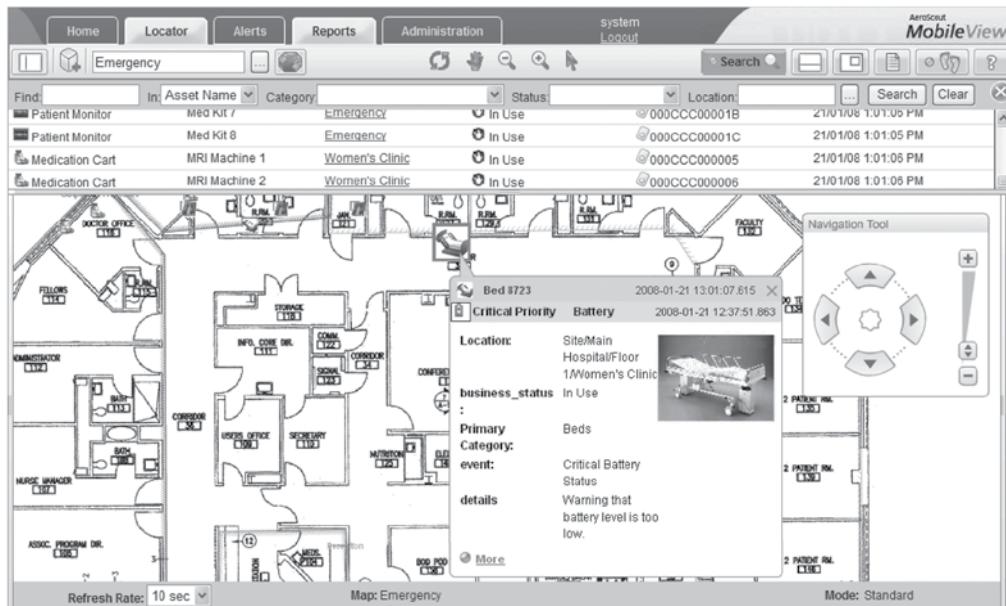
Активные метки RFID и/или стандартные устройства Wi-Fi передают короткий сигнал с постоянным интервалом, добавляя статус или данные датчика, если нужно. Рисунок 11.20 показывает активную метку RFID, прикрепленную к госпитальному внутривенному инфузионному насосу [hospital IV pump]. Сигнал, полученный стандартными ТД (или датчиками RTLS), не требующие какого-либо изменения инфраструктуры, и отправляется в механизм обработки [processing engine], который находится в сервере RTLS в ядре сети. Сервер RTLS использует алгоритмы силы сигнала и/или времени прибытия, чтобы определить координаты местоположения.

**РИСУНОК 11.20** Активная сетка 802.11 RFID



Как показывает Рисунок 11.21, далее используется интерфейс программного обеспечения для просмотра местоположения и состояния на карте поэтажного плана здания. Приложение RTLS может отображать карты, позволяет искать, автоматически оповещать о тревогах, вести учет имущества, и взаимодействовать со сторонними приложениями. Стоит отметить, что решения RTLS также используют и другие радиотехнологии, например Bluetooth с низким энергопотреблением [Bluetooth Low Energy (BLE)] и Ультра Широкий Диапазон

**РИСУНОК 11.21** Приложение RTLS



## VoWiFi

Связь VoIP [голос поверх IP] существует много лет в проводных сетях. Однако, использование VoIP на беспроводных ЛВС 802.11 представляет много вызовов из-за радио среды и параметров, которые нужно учесть, по поводу QoS. В последние годы, запрос на решения Голоса поверх Wi-Fi [Voice over Wi-Fi (VoWiFi)] значительно вырос. БЛВС может быть использована для обеспечения связи для всех данных приложений и в тоже самое время обеспечивать голосовую связь, используя ту же самую инфраструктуру БЛВС. Компоненты, необходимые для развертывания решения VoWiFi включают следующее:

**Телефоны VoWiFi** Телефон VoWiFi похож на сотовый телефон, кроме того, что радиомодуль – это радиомодуль 802.11 вместо сотового радиомодуля. Телефоны VoWiFi являются клиентскими станциями 802.11, которые работают через точку доступа. Они полностью поддерживают шифрование WEP, WPA, и WPA2, и возможности качества сервиса WMM [WMM QoS]. Рисунок 11.22 показывает 84 серию телефонов VoWiFi компании Спектралайнк [Spectralink], у которых есть радиомодуль 802.11a/b/g/n и могут работать в 2,4 ГГц или 5 ГГц полосе. Технология VoWiFi может также располагаться в форм факторе отличном от телефона.

Как изображено на Рисунке 11.23, производитель VoWiFi Vocera продаёт носимые рации со связью по 802.11. Рации Vocera являются полнофункциональными телефонами VoWiFi, в которых также есть распознавание голоса и программное обеспечение верификации голоса. Носимые VoWiFi рации активно используются докторами и медсёстрами в больницах. На текущий момент большинство решений VoWiFi используют Протокол Установления Сеанса Связи [*Session Initiation Protocol (SIP)*] в качестве сигнального протокола для голосовой связи поверх IP сети.

#### РИСУНОК 11.22 VoWiFi телефон (Spectralink 84-Series VoWiFi phone)

Любезно предоставлено компанией Спектралайнк [Spectralink]



#### Инфраструктура 802.11(ТД и Контроллеры)

Существующая инфраструктура БЛВС используется для связи 802.11 между VoWiFi и точками доступа. Могут использоваться решения с отдельно стоящей ТД и/или решение с контроллером БЛВС.

#### УАТС [PBX]

Учреждёнская Автоматическая Телефонная Станция (*УАТС*) [*private branch exchange (PBX)*] это телефонный коммутатор, который обслуживает определенное предприятие или офис. PBXs создают соединения между внутренними телефонами частной компании, а также соединяют их с *Телефонной Сетью Общего Пользования (ТСОП)* [*public switched telephone network (PSTN)*] транковыми линиями. УАТС [PBX] обеспечивает тоновый набор и может предоставить другие функции, например голосовую почту.

**Поддержка WMM** Как обсуждалось в ранних главах, механизмы WMM нужны, чтобы соответствующим образом поддержать QoS.

**FIGURE 11.23** VoWiFi Рации в виде бэджей[ badges] компании Vocera

Любезно предоставлено компанией Восера [Vocera]



## Облачные Сети

Наверное, самые модные термины на текущий момент в ИТ индустрии - это облачные сети, машинное обучение, и искусственный интеллект. Как упоминалось ранее в этой главе, решения NMS доступны из облака как услуга подписки на программное обеспечение. Большая часть поставщиков сетей для предприятий предлагает облачную услугу по управлению и мониторингу проводных и беспроводных сетей.

*Облачные вычисления [Cloud computing]*- доступные по запросу [on-demand] ресурсы вычислительной (компьютерной) системы, хранилище данных, и вычислительная мощность без прямого пользовательского управления. Термин в основном используется для описания центров обработки данных [data centers] доступных многим пользователям через Интернет. Самые большие [Top-tier] провайдеры облачных услуг предлагают эти ресурсы по всему миру с надежными уровнями резервирования, встроенными в региональные центры обработки данных (датацентры). Три самых крупных облачный провайдера это Веб Сервисы Amazon [Amazon Web Services (AWS)], Microsoft Azure, и Облако Google [Google Cloud].

За последние пять лет тенденции в ИТ-индустрии развивались вокруг облачных вычислений и сетей. Компании теперь нанимают специалистов по облачным технологиям для своих DevOps команд, а сотрудники с облачной экспертизой в большом спросе. Длительное обсуждение облачных технологий находится очень далеко за пределами данной книги. Однако, мы будем обсуждать облака применительно к управлению БЛВС.

*Облачные сети [Cloud networking]* описывают где сетевые возможности и ресурсы доступны по запросу через сторонний сервис, который размещает их на облачной платформе. Как ранее упоминалось, решения NMS доступны в облаке как услуга подписки на программное обеспечение.

Существует три основных типа моделей облачного сервиса:

- **Инфраструктура как Услуга [Infrastructure as a Service (IaaS)]:** Поставщики облачных услуг, такие как AWS и Google, предлагают хранение данных, вычислительные мощности [computing], и сетевые ресурсы как размещаемое [hosted] предложение. Заказчики, такие как корпоративные сетевые компании, платят за эти сервисы на основе использования; однако, заказчик все еще отвечает за создание любого приложения поверх инфраструктуры.
- **Платформа как Услуга [Platform as a Service (PaaS)]:** Облачные поставщики услуг, такие как AWS и Google, предлагают услуги управляемых платформ, чтобы сделать разработку приложений легче. PaaS объединяет вместе вычислительные услуги и другие решения, которые обеспечивают более доступную структуру [framework] для разработки приложений. Может быть предложено несколько платформ, включая базы данных, контейнеры, инструменты машинного обучения, услуги сообщений [messaging], оркестрации и т.д.
- **Программное обеспечение как Услуга [Software as a Service (SaaS)]:** Приложения построены поверх облачной инфраструктуры и предлагаются как сервис подписки. Типовые примеры - это Microsoft Office 365 и Salesforce. Корпоративные сетевые компании предлагают теперь свои приложения NMS как сервис по подписке для управления и мониторинга проводных и беспроводных сетей.

Облачные сети с годами развивались. Первое поколение приложений NMS предлагаемого в качестве облачного решения управления были монолитными приложениями, которые работали на нескольких виртуальных машинах [virtual machine (VM)] в центре обработки данных [data center]. Текущие поколения решений NMS построены на платформах провайдеров, таких как Amazon, Google, или Microsoft. Более того, приложения NMS более не являются монолитными, а вместо этого построены на микросервисах [microservices]. Вы готовы к еще нескольким модным облачным терминам?

*Микросервисы [Microservices]* - так называется техника проектирования программного обеспечения, в которой приложение разбито на небольшие операционные части с четко определенными функциональными границами. Микросервисы используются, чтобы сделать структуру приложения как набор нежестко связанных сервисов, связанных вместе через программируемый интерфейс приложения [application programming interfaces (APIs)]. Преимущество микросервисного облачного приложения в том, что программное обеспечение, разбитое на небольшие модули и сервисы, приводит к долговечности и масштабируемости. В отличии от традиционных монолитных приложений, каждый индивидуальный микросервис может быть установлен, настроен, и переустановлен независимо, без подвергания риску целостности приложения.

*Контейнеры [Containers]* - это облегченная альтернатива виртуальной машине [virtual machine (VM)], которая включает инкапсуляцию приложения в контейнер со своей операционной системой. Работающее программное обеспечение в контейнеризированной среде обычно использует меньше пространства и памяти, чем работающее приложение в различных VM. Докер [Docker] - это платформа с открытым исходным кодом для работающих контейнеров. Микросервисная архитектура часто состоит из многих

контейнеризированных микросервисов для работы приложения. Не является чем-то необычным иметь свыше 40 различных сервисов, которые могут быть одним контейнером, коллекцией контейнеров, или распределенным набором контейнеров.

Облачные архитектуры опираются на уровень оркестрации для контроля динамической установки, работы и масштабирования контейнеров. *Оркестрация [Orchestration]* управляет соединениями между микросервисами, контейнерами, другими облачными системами, и промежуточными системами и ПО [middleware]. Оркестрация автоматизирует многое из обеспечения [provisioning], мониторинга, и масштабирования контейнеров. Кубернетес [Kubernetes] – это система с открытым исходным кодом для оркестрации контейнеров, но существуют и другие варианты и инструменты.

Еще одно преимущество использования облачной экосистемы – это сбор данных, хранение данных, и анализ данных в неограниченном масштабе, который был бы никогда невозможен с традиционными системами баз данных. *Большие данные [Big data]* это фраза, часто используемая для описания огромных, разнообразных наборов информации, которые растут с постоянно увеличивающейся скоростью. Данные, собранные и отправленные в облачную архитектуру, могут прийти из разных источников и разным транспортом.

Например, сетевые устройства, такие как ТД и коммутаторы могут непрерывно отправлять метаданные о подключенных беспроводных и проводных клиентах. Как видно на информационной панели облачной NMS одного производителя, показанной на Рисунке 11.24 , что свыше 5 Петабайт данных собирается примерно с 1 миллиона сетевых устройств ежедневно.

В перспективе, 1 Петабайт данных равен 13,3 годам HD видео. Следовательно, каждый день, эта облачная архитектура обрабатывает данные эквивалентные 67 годам HD видео.

**РИСУНОК 11.24** Большие данные в облаке [Big data in the cloud]

Courtesy of Extreme Networks



Помните, что эти данные – это метаданные с сетевой информацией. Пользовательский трафик не посыпается в облако, только трафик управления. Точки доступа, коммутаторы, и

другие сетевые устройства часто посылают метаданные с одноминутными интервалами. Однако, некоторые метаданные, такие как изменения в сессии Wi-Fi клиента (пример: роуминг), посылаются в облако мгновенно. Множество протоколов, таких как HTTPS, CAPWAP, и MQTT могут безопасно переправить метаданные от устройства в облако.

Облачная архитектура необходима для сбора, обработки и анализа огромного количества сетевых и генерируемых клиентами данных, а затем перевести их в наглядный и действенный вид для ИТ департаментов. Как изображено на Рисунке 11.25, облачная NMS может предоставить состояние в реальном времени и историческом сетевых устройств, клиентов, и пользователей всей сети.

**РИСУНОК 11.25** Состояние сети [Network Visibility]



Следующий шаг в предоставлении глубокого понимания и лучшего отображения сетевых операций - это машинное обучение [*machine learning*]. В облаке, алгоритмы машинного обучения используют тренировочные данные, чтобы строить математические модели, которые описывают данные; затем модели применяются к рабочим данным, чтобы решить потенциальные сетевые проблемы. Облачная NMS может использовать машинное обучение, чтобы установить базовые уровни касательно производительности Wi-Fi, обнаружить аномалии, и автоматизировать некоторые аспекты поиска и устранения сетевых проблем [network troubleshooting]. Например, обнаруженная аномалия может запустить автоматическую сборку пакетов Wi-Fi на точке доступа. Анализ причин может помочь сетевым администраторам в локализации сетевых проблем. Огромное количество наборов данных является требованием для улучшения точности машинного обучения. Облачные решения NMS стали поддерживать растущую тенденцию по использованию машинного обучения для управления беспроводными и проводными сетями.

# Программируемый Интерфейс Приложения

Десятилетиями, системные инженеры в ИТ используют интерфейс командной строки [*command-line interface (CLI)*] или *графический пользовательский интерфейс* [*graphical user interface (GUI)*] для взаимодействия с физическими сетевыми устройствами для того, чтобы изменить конфигурацию устройства, проверить его работу [monitor], или для поиска и устранения проблем [troubleshooting]. CLI был традиционно предпочтительным методом для сетевых инженеров. Надежность CLI часто была ключевым фактором, когда приобреталось новое сетевое оборудование. При условии, что они были знакомы с CLI, сетевые инженеры могли быстро настроить сетевой узел вместо использования графического интерфейса (GUI). Сетевые инженеры могли копировать, редактировать и вставлять конфигурационные команды между устройствами. Также, создание скриптов [scripts] могло автоматизировать процесс настройки и мониторинга сетевых устройств, что увеличивало скорость и масштабируемость развертывания при установке.

Эволюция технологий привела к миграции приложений в облако. Этим облачным приложениям нужно извлекать данные и взаимодействовать с корпоративной сетью. Старые системы управления сетью так же, как и системы операционной поддержки/системы поддержки бизнеса [*operations support system/business support systems (OSS/BSS)*] взаимодействуют с сетевой инфраструктурой, используя стандартные протоколы управления, такие как SNMP. Однако, эти протоколы управления не были разработаны для масштабирования в эру облаков, и редко проектировались для двусторонней связи.

Сегодня, приложениям, которым нужно взаимодействовать с сетью, больше не ограничены небольшой группой пользователей, как сетевые инженеры и администраторы. Приложения, такие как системы гостевого управления, розничная аналитика [*retail analytics*], и другие аналитические движки, все требуют своего рода прямое взаимодействие с сетью. Взаимодействие часто двунаправленное, и используется для настройки сети и получения данных сетевого мониторинга. По факту, с ростом устройств Интернета Вещей [*Internet of Things (IoT)*], некоторые из этих приложений не взаимодействуют с пользователями, и вместо этого, взаимодействуют только с другими приложениями. Чтобы позволить этим приложениям взаимодействовать друг с другом, нужен *программируемый интерфейс приложения* [*application programming interface (API)*]. API - это набор подпрограммных определений, протоколов, и инструментов для построения программного обеспечения.

## Транспорт и Форматы Данных

API позволяет приложениям взаимодействовать с другими приложениями, для того чтобы обмениваться данными и выполнять задачи. Например, если в розничном магазине и хотели бы использовать приложение на вашем смартфоне, чтобы направить вас к вашему любимому бренду обуви, приложению нужно будет взаимодействовать с системой аналитики местоположений [*location analytics*], чтобы определить ваше текущее местоположение. Данные о вашем местоположении приходят из БЛВС, хранятся в системе по аналитике местоположений, и запрашиваются приложением на вашем смартфоне. Для разработки приложений, API заменили CLI, но следуют похожему набору правил. API оценивается на основе его простоты, производительности и полноты, а это означает, что многие функции, поддерживаемые системой, доступны через API.

Так же как CLI требует транспортный протокол, такой как SSH, чтобы подключить

пользователя к устройству, так и APIs требуют транспортный протокол, чтобы соединиться с другими приложениями. Наиболее общим транспортными протоколами являются HTTP и HTTPS, потому что они поддерживаются широким диапазоном устройств. Обладание такой родной поддержкой устраняет необходимость устанавливать дополнительные библиотеки или разрабатывать новые протоколы, а также это обеспечивает безопасность путем поддержки шифрования с использованием SSL. Это обеспечивает безопасный канал между различными приложениями при обмене данными. *RESTful API* это программируемый интерфейс приложения [application program interface (API)], который использует HTTP запросы GET, PUT, POST, и DELETE.

Данные, сами по себе, могут быть различных форматов, однако наиболее популярный формат называется *Объектная Нотация JavaScript* [*JavaScript Object Notation (JSON)*]. В отличие от других форматов (например, XML), формат JSON является само-описательным и легко читается человеком. Формат JSON определяет пары ключ/значение [key/value], где ключ описывает, что данные означают, а значение - это сами актуальные данные. В дополнение к читаемому человеком, JSON - очень эффективен для транспорта.

## APIs БЛВС

APIs БЛВС может быть категоризировано на три группы:

**Конфигурационные [Configuration] APIs** APIs могут быть использованы для изменения конфигурационных настроек ТД или других сетевых устройств.

Конфигурационные APIs могут быть использованы для таких простых вещей как создание нового набора учетных данных пользователя БЛВС, или более сложных настроек, таких как создание нового SSID с VLANом и политиками доступа с QoS.

**Мониторинговые [Monitoring] APIs** APIs могут быть использованы для получения данных сетевой статистики, таких как состояние ТД, использование CPU и памяти, счетчики трафика, и т.д. Мониторинговые APIs могут также быть использованы для получения данных мониторинга для клиентских устройств БЛВС, таких как время соединения, роуминговые события, IP адреса, и используемые приложения.

**Уведомительные [Notification] APIs** Оповестительные или Нотификационные APIs, более часто называемые вебхук *[webhook]* APIs, предлагают сервис подписки, где приложение может подписаться на получение уведомлений, когда происходит определенное событие. Вебхук APIs запускается по событию. Например, когда система обнаруживает, что ТД больше не отвечает, она отправляет сообщение с указанием ID устройства, временной отметки, и других данных подписавшемуся приложению.

И конфигурационные, и мониторинговые APIs могут считаться синхронными. Приложение, которому требуются данные для начала изменения конфигурации, вызывает API. Система, получающая вызов API, отвечает набором данных или просто возвращает результат выполнения операции (т.е.: изменение конфигурации - "успешно" [*configuration change is "success"*]). Однако, этот тип API вызова не подходит для оповещений.

Например, чтобы запустить действие, когда точка доступа больше не отвечает, будут нужны непрерывные вызовы к мониторинговому API, чтобы отсортировать из всего списка ответивших ТД, и отфильтровать ТД, которые больше не подключены. Этот подход API называется опросом *[polling]* и считается тратающим в пустую системные ресурсы. Вебхук *[Webhook]* APIs вместо этого запускаются по событию, и опрос *[polling]* не нужен.

Использование вебхук *[webhook]* APIs для оповещений уменьшает загрузку системы и минимизирует поток трафика между приложениями.

## Типовые Приложения

Одно из наиболее распространенных приложений, которое использует API в БЛВС, это система управления сетью (NMS). Почти все облачные решения NMS предлагают внешние API для сетевого управления и мониторинга. NMS собирает мониторинговые данные с различных устройств БЛВС и представляет данные, используя информационные панели, графики, и другие техники визуализации. NMS может использовать собранные данные для анализа типового поведения, установки базовых параметров, и наблюдения за аномалиями. Более продвинутые NMS могут использовать предиктивную аналитику для предсказания будущих событий или сбоев, используя собранные данные. Поддерживаемая конфигурационными API NMS может проактивно адаптировать конфигурацию БЛВС для предотвращения сбоев и перегрузки, и назначать соответствующий QoS определенным клиентским устройствам и приложениям.

Другое распространенное использование API в БЛВС - это аналитика местоположения [location analytics]. БЛВС являются богатым источником данных местоположения, таких как физическое распределение устройств по этажу в течении дня, время пребывания клиентов, или даже отслеживания местоположения людей и имущества в режиме реального времени. Количество таких данных, созданных крупными корпоративными БЛВС, могут быть ошеломляющими. Для обработки и предоставления таких данных требуются методы, которые позволяют быстро анализировать и сохранять данные, не перегружая NMS. Хорошо описанный и внедренный API может помочь получить данные местоположения, а также анализировать и сохранять быстрорастущие наборы данных.

API местоположения также можно использовать, чтобы помочь приложению на вашем смартфоне внести дополнительный контекст в физическое пространство, в котором вы сейчас стоите. Например, API аналитики местоположения может запустить приложение на мобильном устройстве, чтобы показать интерактивное содержание (контент), когда посетитель находится в непосредственной близости от музеяного экспоната. Этим решениям на основе близкого расположения [proximity-based solutions] часто помогают другие радиотехнологии такие как *Bluetooth с низким энергопотреблением [Bluetooth Low Energy (BLE)]* и *ультра широкий диапазон [ultra-wideband (UWB)]*, которые обсуждаются в Главе 20 "Установка БЛВС и Вертикальные Рынки".

Заказчики производителей Wi-Fi, партнеры и поставщики управляемых услуг [managed service providers (MSPs)] стали использовать API производителей, чтобы строить свои собственные пользовательские приложения для мониторинга беспроводных и проводных сетей. Пользовательские приложения также могут быть построены для конфигурации устройств и оповещений. Некоторые из крупнейших сетевых производителей поддерживают портал сообщества разработчиков как репозиторий документации по API, примеров кода, и справочные приложения. С появлением облачной технологии корпорации используют API для удовлетворения растущих потребностей в отображении, анализе и хранении сетевых данных.

## Управление Инфраструктурой

Совершенный дизайн сети предписывает размещать сетевые устройства в выделенных VLANах управления или других внеполосных [out-of-band] интерфейсах, чтобы изолировать их от обычного сетевого трафика. Сетевые устройства уровня предприятия должны предоставлять эту функциональность для того, чтобы инфраструктурные устройства были недоступны для хакеров или даже для сотрудников, которые могут получить доступ к сети.

По мере того, как размер сетей БЛВС [WLAN] с годами рос, росли и вызовы управления ими. Они включают управление следующими пунктами:

- Версии ПО и прошивки [Firmware revisions]
- Конфигурации и изменения [Configurations and changes]
- Мониторинг и реакция на инциденты [Monitoring and incident response]
- Управление и фильтрация сигналов тревоги и предупреждений от устройств [Managing and filtering of device alerts and alarms]
- Мониторинг производительности [Performance monitoring]

Чтобы сделать работу по управлению этими устройствами легче, обычно стандартные

сетевые протоколы для управления устройствами включаются в большую часть оборудования БЛВС, и может быть интегрировано с программными системами управления, которые могут охватывать даже самые большие сети. Чем больше система сетевого управления (NMS) вовлечена в сетевую структуру, тем меньше времени тратиться на выполнение рутинных задач по поддержке сети. Без исключения, каждый раз, когда NMS корректно внедрена, удовлетворенность пользователей сети выше, а операционные затраты на сеть ниже. Не менее важно проведение установки NMS в рабочую среду с сотрудниками поддержки. Разработка процессов и процедур вокруг таких систем, и делая их частью ежедневной работы персонала поддержки также являются критичными.

## Протоколы Управления

Существует много различных типов протоколов, используемых для управления сетевыми устройствами. Простой Протокол Сетевого Управления [Simple Network Management Protocol (SNMP)] существует уже достаточно долго и претерпел несколько переработок. В дополнение к SNMP, большинство устройств может быть настроено с использованием интерфейса командной строки [command-line interface (CLI)] или графического пользовательского интерфейса [graphical user interface (GUI)].

Следующие протоколы являются общепринятыми для управления БЛВС. Некоторые из этих протоколов основаны на де-юре стандартах, а некоторые базируются на де-факто стандартах. В любом случае они предоставляют основу для управления и администрирования БЛВС.

### SNMP

*Простой Протокол Сетевого Управления [Simple Network Management Protocol (SNMP)]* это протокол Прикладного уровня (7ой уровень OSI), используемый для прямого взаимодействия с сетевыми устройствами. SNMP позволяет получать (дословно – вытягивать) [pulling] информацию из устройства, а также отправлять (дословно – заталкивать) информацию на центральный SNMP сервер на основе определенных, часто настраиваемых пользователем, порогов на сетевых устройствах. Отправка [push] из устройства может включать сообщение относительно возврата в исходное состояние (сброса) интерфейса, высокого количества ошибок, высокой утилизации сети или CPU, сигнализация безопасности, и многие другие критические факторы связанные со нормальной работой и состоянием устройств.

### Компоненты

Система управления по SNMP содержит следующее:

- Несколько (потенциально много) узлов, каждый с SNMP объектом [entity] (а-ля агент), содержащий приложения по *ответам на команды [command responder]* и *отправлению уведомлений [notification originator]*, которые имеют доступ к инструментам управления
- По крайней мере один SNMP объект, содержащий приложения по созданию команд [command generator] и/или получению уведомлений [notification receiver] (традиционно называемого менеджером [manager])
- Протокол управления, используемый для передачи управляющей информации между SNMP объектами.

### Структура Информации Управления

Информация управления структурирована в виде коллекции управляемых

объектов, содержащихся в базе данных, называемой *база информации управления [management information base (MIB)]*.

MIB состоит из следующих определений: модули [modules], объекты [objects], и ловушки [traps]. Определения модулей используются при описании информационных модулей. Определения объектов используются при описании управляемых объектов. Описание ловушек [Trap] являются уведомлениями, используемыми для незапрошенной передачи MIB информации, обычно в NMS. У всех устройств с поддержкой SNMP есть MIB, и в этой MIB должна находиться конфигурация и статус устройства. Однако, производители обычно не полностью доделывают свои MIB и внедрение SNMP. Часто вы найдете, что определенные части критичной информации недоступна через SNMP, а, следовательно, ловушки [traps] не могут быть внедрены с использованием этой информации.

## Версии и Различия

SNMP претерпел множество переделок за годы своего существования. Этот раздел не предназначен быть полной историей SNMP, а скорее обзором, чтобы направить вас к пониманию различий между различными версиями. Дополнительно, этот раздел поможет вам соответствующим образом применять различные версии в вашем сетевом дизайне путем понимания сильных сторон и того как обращаться со слабыми сторонами.

### SNMPv1

Версия 1 SNMP вышла на сцену в 1988 году. Как многие другие изначальные нововведения протоколов, SNMPv1 не был совершенным с первого раза. SNMPv1 был спроектирован для работы через широкий диапазон протоколов, использовавшихся в то время, включая IP, UDP, CLNS, AppleTalk и IPX—но наиболее распространенное использование с UDP.

SNMPv1 использовал строку *сообщества* [*community string*], которую должен был знать удаленный агент. Так как SNMPv1 не применял никакого шифрования, он был объектом перехвата пакетов, чтобы найти строку сообщества, указанную открытым текстом. Следовательно, SNMPv1 был сильно критикуем за небезопасность. Эффективность протокола также была недостаточной для этого начального представления протокола. Каждый объект MIB должен был быть получаем по очереди один за одним в итеративном стиле, что было очень неэффективно.

### SNMPv2

Когда был выпущен SNMPv2, несколько областей были переработаны, включая производительность, безопасность и взаимодействие менеджер-менеджер. Производительность протокола стала более эффективной с введением новых функций таких как GETBULK, которая решала проблему итеративного метода извлечения большого количества данных из MIBs.

Безопасность была улучшена путем определения новой системы безопасности на основе сторон [*party-based security system*]. Критики упрекали систему на основе сторон за избыточную сложность, и система не получила широкого распространения.

Позднее был определен SNMPv2c в RFCs 1901–1908 и называется как версия *на основе строки сообщества* [*community-based version*]. Страна сообщества [*community string*] из SNMPv1 была принята в SNMPv2c, что, по сути, отменило все улучшения безопасности протокола. SNMPv2c не применяет шифрование и является объектом для перехвата пакетов со строкой сообщества в открытом виде.

### SNMPv3

Большое количество функций безопасности было добавлено в SNMPv3, включая следующее:

- Аутентификация выполняется с использованием SHA или MD5.
- Конфиденциальность—SNMPv3 использует шифрование DES 56-bit, основанное на

- Контроль доступа—Используются пользователи и группы, каждый с различными уровнями привилегий. Имя пользователя и пароль заменяют строку сообщества [community strings].

Хотя эти функции являются опциональными, обычно основной движущей силой за внедрение SNMPv3 является получение этих функций безопасности. Опциональным также является безопасная аутентификация, но без шифрования.

Даже с этими функциями большинство сетевых дизайнеров все еще считают, что лучше включать SNMP Агенты только на безопасных интерфейсах управления. А именно, разделение по VLANам и фильтрация межсетевым экраном обычно выполняется со всем SNMP трафиком к сетевым устройствам. Ни один достаточно сложных протокол не считается полностью безопасным, и дополнительная защита всегда очень рекомендована. Если вы собираете внедрить NMS с использованием SNMP, мы настойчиво рекомендуем, чтобы вы использовали SNMPv3. Один из наиболее важных вопросов безопасности в том, что большинство производителей оборудования на заводе включают SNMP, со строкой сообщества [community string] на чтение [read] и запись [write] с заводскими значениями. Это *огромная* угроза безопасности для конфигурации и работы вашей сети, и одним из первых шагов должна быть по блокировка этого для защиты сетевых устройств.

## Управление на основе CLI (командной строки)

Интерфейсы командной строки [Command-line interfaces (CLIs)] являются одним из множества распространенных способов, используемых для настройки и управления сетевыми устройствами. Кажется, что вековые споры GUI [графический интерфейс] против CLI [командной строки] все еще имеют место быть по сей день и врядли изменятся в ближайшее время. Графические интерфейсы [GUIs] выполняют прекрасную работу по представлению информации, но из-за браузерной несовместимости, ошибок JavaScript, ошибок[bugs] в ПО GUI, временных задержках, и другого, GUI все еще сподвигает многих людей вернуться обратно к командной строке.

CLIs работают с необработанной, неотредактированной конфигурацией устройств и предоставляют возможность сделать быстро определенные изменения в конфигурации устройств. Команды, вводимые через CLI, могут даже быть запрограммированы (т.е. записаны в виде скрипта), позволяя выполнить начальную конфигурацию устройства или даже переконфигурацию простым копированием [copy] и вставкой [paste] во время сеанса CLI.

Командные строки [CLIs] могут быть доступны, используя несколько способов, которые зависят от используемого устройства. Эти типовые способы – это:

- Последовательный и консольный порты
- Телнет [Telnet]
- SSH1/SSH2

## Последовательный и Консольный Порты

Интерфейсы последовательного [serial] или консольного [console] порта могут различаться от производителя к производителю и даже от модели к модели. Это чрезвычайно мешает сетевым инженерам. Некоторые из них используют стандартный интерфейс с последовательным DB-9 разъемом, в то время как другие используют интерфейс RJ-11 или RJ-45. Более того, подходящий кабель может иметь проприетарную распиновку [pin-out] (особенно для разъемов RJ-11 и RJ-45), нуль-модемный кабель [NULL-modem cable], перекрученный кабель [rollover cable], или прямой кабель [straight-through cable]. Скорость в бодах [baud], число бит, контроль потока [flow control], четность [parity], и

другие параметры также варьируются от устройства к устройству.

Не важно какой тип разъема или кабеля вы используете для управления вашим сетевым устройством, последовательный или консольный порты должны быть заблокированы и требовать механизм аутентификации пользователя. Хотя обычно это может быть преодолено путем процедуры восстановления пароля [password-recovery routine], используя инструкции, которые можно быстро найти в Интернете, механизм пользовательской аутентификации поможет задержать хакеров. Обычно, устройства требуют перерыв в работе, чтобы восстановить пароль, и влияние отсутствия сервиса может быть достаточным, чтобы предупредить персонал о попытке физического "взлома" сетевых устройств. Важно отметить, что большинство процедур восстановления пароля требуют прямого доступа к устройству по серийному [serial] или консольному [console] порту. Установка сетевого оборудования в закрытом коммутационном шкафу или аппаратном зале поможет предотвратить этот тип атак.

Государственное регулирование такое как FIPS 140-2 может требовать, чтобы последовательный [serial] и консольный [console] порты были защищены этикеткой с контролем вскрытия [tamper-evident label (TEL)], чтобы предотвратить неавторизованный физический доступ к устройству инфраструктуры БЛВС, такого как контроллер БЛВС. Этикетки с контролем вскрытия [TELs] не могут быть незаметно разорваны, удалены или перенаклеены без очевидных видимых изменений. Как показано на Рисунке 11.26, каждая этикетка [TEL] имеет уникальный серийный номер, для предотвращения замены на похожую этикетку.

**РИСУНОК 11.26** Этикетка с контролем вскрытия



## Telnet

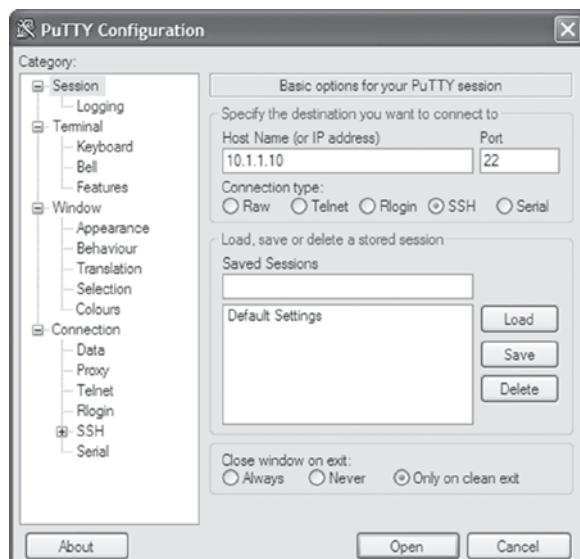
Telnet - еще один протокол, который обычно используется, но часто он может быть использован только после настройки последовательного порта или первоначальной настройки из заводского состояния. Обычно на устройстве должен быть включен IP для того, чтобы оно было доступно и было управляемо через сетевой интерфейс.

Telnet сильно критикуем и обычно запрещен к использованию корпоративными политиками безопасности из-за отсутствия шифрования. Telnet - совершенно нешифруемый протокол, и полезная нагрузка каждого пакета может быть просмотрена при перехвате пакета. Это включает имя пользователя и пароль во время последовательности входа в систему. Мы рекомендуем, чтобы вы выключали Telnet после первоначальной настройки устройства. У большинства компаний есть прописанные политики предписывающие, чтобы Telnet был выключен.

## Secure Shell

*Безопасная Оболочка [Secure Shell (SSH)]* обычно используется в качестве безопасной альтернативы Телнету. SSH применяет аутентификацию и шифрование с использованием шифрования с открытым ключом [public-key] всего сетевого трафика проходящего между хостом [host] и пользовательским устройством. Возможности Telnet для управления на основе командной строки [CLI] применимы к SSH, но включают еще функции безопасности. SSH протоколу назначен стандартный TCP порт 22. Большинство устройств БЛВС инфраструктуры сейчас поддерживают вторую версию SSH протокола, называемую *SSH2*. В соответствии с политикой, когда устройства БЛВС управляются через CLI, следует использовать программы эмуляции терминала с поддержкой SSH2. Рисунок 11.27 показывает конфигурационный экран популярной свободно распространяемой программы PuTTY, которая поддерживает SSH2.

**РИСУНОК 11.27** Свободно распространяемое ПО PuTTY клиент SSH2



## HTTPS

Безопасный Протокол Передачи Гипертекста [Hypertext Transfer Protocol Secure (HTTPS)] является комбинацией Протокола Передачи Гипертекста [Hypertext Transfer Protocol] с протоколом SSL/TLS для обеспечения шифрования и безопасной идентификации. HTTPS - это фактически SSL сессия, которая использует HTTP и внедрена на сетевых устройствах для управления через графический пользовательский интерфейс (GUI). Не все пользователи предпочитают управление через командную строку (CLI), а графический интерфейс (GUIs) в основном используется там, где используется NMS для управления инфраструктурой БЛВС.

Так как HTTP передается открытым текстом, он уязвим для перехвата и атакам "человек посередине" [man-in-the-middle] и модификации при передаче. Некоторые устройства предлагают и HTTP и HTTPS, но важно, чтобы хотя бы аутентификация осуществлялась через HTTPS. Если пользователи устройств будут входить в графический интерфейс (GUI) без использования HTTPS, то это является чистой халатностью, если устройство поддерживает его.

## ИТОГО

Эта глава обсуждала различные типы форм факторов радиомодулей, их чипсеты, и программные интерфейсы, необходимые для настройки клиентских станций. Мы обсуждали три логические плоскости работы телекоммуникаций, и где они присутствуют в трех наиболее распространенных архитектурах БЛВС. Мы также показали вам логическое развитие, которое сделали устройства БЛВС, начиная от автономных точек доступа, далее двигаясь к контроллерам БЛВС, и затем двигаясь по пути распределенной архитектуры. Так же, мы охватили специальные устройства инфраструктуры БЛВС, которые часто удовлетворяют потребности, которые не могут быть удовлетворены более традиционной архитектурой БЛВС. Мы также описали облачные сети и обсудили как облачное управление и API революционизировало системы управления сетями.



Авторы этой книги рекомендуют вам перед прохождением экзамена CWNA самостоятельно попрактиковаться с некоторыми устройствами инфраструктуры БЛВС. Мы понимаем, что большинство не может позволить себе контроллер БЛВС за 10 000\$ и много ТД; однако, мы рекомендуем вам купить, по крайней мере, один клиентский адаптер 802.11, и или точку доступа или беспроводной маршрутизатор уровня SOHO. Многие производители корпоративных БЛВС также предлагают программу "бесплатной точки доступа" ["free access point"] для потенциальных заказчиков. Практические упражнения закрепят многое из того, что вы узнали в этой главе, а также и из других глав в этой книге.

## Темы Экзамена

**Знать основные форм факторы радиомодулей.** Стандарт 802.11 не предписывает какой тип формата может быть использован радиомодулем 802.11. Радиомодули 802.11 существуют во множестве форматов.

**Понимать необходимость клиентским адаптерам иметь интерфейс операционной системы и пользовательский интерфейс.** Клиентский адаптер требует специальный драйвер для взаимодействия с операционной системой и программной утилитой для настройки пользователем.

**Определить три логические сетевые плоскости работы** Понимать разницу между плоскостями управления, контроля и данных. Быть способным объяснить где они используются в разных архитектурах БЛВС.

**Понимать типы архитектур БЛВС.** Знать различные типы архитектур, включая автономную, централизованную, распределенную, унифицированную и гибридную. Понимать различные общие характеристики и возможности, которые каждая архитектура предлагает.

**Объяснить роль мостов БЛВС.** Определить разницу между коневым и неконевым мостами. Быть способным объяснить разницу между мостами точка-точка и точка-многоточка. Понимать проблемы мостов, такие как ACK таймаут [ACK timeout], и описать другие доводы о мостах, которые охвачены в других главах, такие как зона Френеля и операционный запас системы.

**Объяснить специальную инфраструктуру БЛВС.** Быть способным объяснить, как RTLS и VoWiFi решения могут быть интегрированы с БЛВС. Объяснить трудгие нетрадиционные решения БЛВС, такие как массивы БЛВС.

**Быть знакомым с характеристиками управления устройствами.** Знать различные способы управления устройствами, характеристики, и доступные протоколы в устройствах БЛВС.

# Контрольные Вопросы

1. Какой термин лучше описывает компоненты централизованной архитектуры БЛВС, где плоскости управления, контроля и данных располагаются в центральном устройстве? (Выберите все, что применимо.)
  - A. Контроллер БЛВС [WLAN controller]
  - B. Система Управления Беспроводной Сетью [Wireless network management system]
  - C. Система Управления Сетью [Network management system]
  - D. Распределенная ТД [Distributed AP]
  - E. ТД, управляемая контроллером [Controller-based AP].
2. Какая логическая плоскость сетевой работы обычно определяется протоколами и интеллектом?
  - A. Плоскость пользователей [User plane]
  - B. Плоскость данных [Data plane]
  - C. Плоскость сети [Network plane]
  - D. Плоскость контроля [Control plane]
  - E. Плоскость управления [Management plane]
3. Какая архитектурная модель БЛВС обычно требует поддержку меток [tagging] 802.1Q на границе сети, когда требуется несколько пользовательских VLANов? (Выберите все что применимо.)
  - A. Автономная архитектура БЛВС [Autonomous WLAN architecture]
  - B. Централизованная архитектура БЛВС [Centralized WLAN architecture]
  - C. Распределенная архитектура БЛВС [Distributed WLAN architecture]
  - D. Ничего из выше указанного [None of the above]
4. Какой тип точек доступа обычно использует централизованную пересылку данных?
  - A. Автономные ТД [Autonomous APs]
  - B. ТД, управляемые контроллером [Controller-based APs]
  - C. Совместно работающие ТД в распределенной архитектуре БЛВС [Cooperative APs within a distributed WLAN architecture]
  - D. Ничего из выше указанного [None of the above]
5. Какие протоколы могут быть использованы для туннелирования пользовательского трафика 802.11 от точек доступа до контроллеров БЛВС или других централизованных серверов? (Примените все, что применимо.)
  - A. IPsec
  - B. GRE
  - C. CAPWAP
  - D. DTLS
  - E. VRRP

6. Какие из этих архитектур БЛВС могут требовать использование сервера NMS для управления и мониторинга БЛВС?
  - A. Автономная архитектура БЛВС [Autonomous WLAN architecture]
  - B. Централизованная архитектура БЛВС [Centralized WLAN architecture]
  - C. Распределенная архитектура БЛВС [Distributed WLAN architecture]
  - D. Все из вышеперечисленного [All of the above]
7. Какой термин лучше описывает централизованную архитектуру БЛВС, где интеграционный сервис (IS) и сервисы системы распространения (DSS) выполняются контроллером БЛВС, а создание определенных кадров 802.11 управления и контроля выполняется ТД, управляемой контроллером?
  - A. Совместноработающий контроль [Cooperative control]
  - B. Распределенная пересылка данных [Distributed data forwarding]
  - C. Распределенная гибридная архитектура [Distributed hybrid architecture]
  - D. Распределенная архитектура БЛВС [Distributed WLAN architecture]
  - E. Разделение контроля доступа к среде [Split MAC]
8. Что является необходимыми компонентами сетевой VoWiFi архитектуры? (Выберите все, что применимо.)
  - A. VoWiFi телефон
  - B. SIP
  - C. Поддержка WMM [WMM support]
  - D. Прокси сервер [Proxy server]
  - E. ATC [PBX]
9. Что является традиционной моделью пересылки данных для пользовательского трафика 802.11, когда развернут контроллер БЛВС?
  - A. Распределенная пересылка данных [Distributed data forwarding]
  - B. Автономная пересылка [Autonomous forwarding]
  - C. Прокси пересылка данных [Proxy data forwarding]
  - D. Централизованная пересылка данных [Centralized data forwarding]
  - E. Все из выше указанного [All of the above]
10. Какие функции безопасности находятся в маршрутизаторе БЛВС уровня предприятия, который обычно устанавливается в удаленном филиале? (Выберите все, что применимо.)
  - A. Встроенный сервер WIPS [Integrated WIPS server]
  - B. Встроенный сервер VPN [Integrated VPN server]
  - C. Встроенный сервер NAC [Integrated NAC server]
  - D. Встроенный межсетевой экран [Integrated firewall]
  - E. Встроенный VPN клиент [Integrated VPN client]

- 11.** Какой форм фактор радиомодуля может быть использован технологией 802.11?
- A.** USB 3.0
  - B.** Secure Digital
  - C.** PCMCIA
  - D.** Mini PCI
  - E.** ExpressCard
  - F.** Проприетарный [Proprietary]
  - G.** Все выше перечисленное
- 12.** Какой из этих протоколов может быть использован для настройки устройств инфраструктуры БЛВС?
- A.** HTTP
  - B.** SSH
  - C.** SNMP
  - D.** Telnet
  - E.** HTTPS
  - F.** SNMP
  - G.** Все выше перечисленные
- 13.** Какие наиболее распространенные возможности архитектуры контроллера БЛВС?
- A.** Адаптивное радио [Adaptive RF]
  - B.** Управление ТД [AP management]
  - C.** Поддержка роуминга 3 уровня [Layer 3 roaming support]
  - D.** Плавное регулирование полосой [Bandwidth throttling]
  - E.** Межсетевой экран [Firewall]
  - F.** Все выше перечисленное
- 14.** Какие протоколы управления часто используются между сервером системы управления сетью (NMS) и удаленными точками доступа для мониторинга БЛВС? (Выберите все, что применимо.)
- A.** IPsec
  - B.** GRE
  - C.** CAPWAP
  - D.** DTLS
  - E.** SNMP
- 15.** Какие распространенные функции безопасности часто интегрированы с точками доступа, развернутыми в распределенной архитектуре БЛВС.?
- A.** Перехватывающий веб портал [Captive web portal]
  - B.** Межсетевой экран [Firewall]

- C.** Встроенный RADIUS [Integrated RADIUS]
  - D.** WIPS
  - E.** Все выше перечисленное
- 16.** Какую радиотехнологию используют клиентские IoT устройства для связи?
- A.** Wi-Fi
  - B.** Bluetooth
  - C.** Zigbee
  - D.** Все из вышеперечисленного
- 17.** Какой тип форм фактора радиомодуля 802.11 обычно используется в мобильных устройствах, таких как смартфоны и планшеты?
- A.** Интегрированный единий чип (микросхема) [Integrated single chip]
  - B.** PCMCIA
  - C.** Экспресс Мини PCI [Express Mini PCI]
  - D.** Мини PCI [Mini PCI]
  - E.** Secure Digital
- 18.** Где нужна избыточность/резервирование [redundancy], если пользовательский трафик теннилируется в централизованной архитектуре БЛВС?
- A.** Резервные радиомодули [Redundant radios]
  - B.** Резервные контроллеры [Redundant controllers]
  - C.** Резервные коммутаторы доступа [Redundant access switches]
  - D.** Резервные точки доступа [Redundant access points]
  - E.** Ничего из выше перечисленного. [None of the above]
- 19.** Какие форм факторы решений системы сетевого управления (NMS) доступны? (Выберите все, что применимо.)
- A.** Аппаратная платформа [Hardware appliance]
  - B.** Виртуальная платформа [Virtual appliance]
  - C.** Сервис облачной подписки [Cloud subscription service]
  - D.** Интегрированная точка доступа [Integrated access point]
- 20.** Какая плоскость работы располагается в точке доступа распределенной архитектуры БЛВС? (Выберите все, что применимо.)
- A.** Плоскость радио [Radio plane]
  - B.** Плоскость данных [Data plane]
  - C.** Плоскость сети [Network plane]
  - D.** Плоскость контроля [Control plane]
  - E.** Плоскость управления [Management plane]

# Глава 12



## Питание по Ethernet (PoE)

---

В ЭТОЙ ГЛАВЕ ВЫ УЗНАЕТЕ О СЛЕДУЮЩЕМ:

✓ История PoE

- Нестандартное PoE
- IEEE 802.3af
- IEEE Std 802.3-2005, Статья 33
- IEEE 802.3at-2009
- IEEE Std 802.3-2018, Статья 33
- IEEE Std 802.3bt

✓ Устройства с PoE

- Питаемое устройство (PD)
- Оборудование подачи питания (PSE)
- Конечное оборудование подачи питания [Endpoint PSE]
- Промежуточное оборудование подачи питания [Midspan PSE]

✓ Планирование и развертывание PoE

- Планирование питания
- Резервирование
- Понижение возможностей PoE
- Доводы по мощности 802.3bt



В этой главе, вы узнаете о различных способах, которыми может быть использован кабель Ethernet для подачи питания сетевым устройствам. *Питание по Ethernet [Power over Ethernet (PoE)]* не является технологией Wi-Fi, и используется не только для Wi-Fi устройств. Однако,

оно стало преобладающим способом подачи питания для точек доступа уровня предприятия, делая таким образом его необходимой и важной темой при обсуждении беспроводных сетей.

## История PoE

Первоначально, компьютерная сеть подразумевала подключение стационарной, запитанной электричеством, компьютерной системы к проводной сети. Компьютерами было все от настольного ПК до серверов и мейнфреймов (больших ЭВМ). Как обычно это бывает с технологиями, огромные компьютеры дали дорогу небольшим компьютерам, и стали появляться ноутбуки и портативные устройства. В конце концов, некоторые сетевые устройства стали достаточно компактными и физически и электронно, так что стало возможным и практичным использовать Ethernet кабель не только для передачи данных к устройству, но также и подавать необходимое питание устройству.

Концепция подачи питания от сети переносит нас к рождению телефона, который в наши дни все также получает питание от телефонной сети. Устройства компьютерной сети, которые часто запитываются по PoE, являются настольными телефонами VoIP (голос по IP), видеокамерами, и точками доступа. Ethernet кабели состоят из четырех пар проводов. В 10 Мбит/с и 100 Мбит/с Ethernet, две пары используются для передачи и получения данных, а другие две пары не используются. Gigabit Ethernet использует все четыре пары проводов для передачи и приема данных. Как вы увидите позже в этой главе, это не проблема, поскольку PoE может обеспечить питание по неиспользуемым проводам или по тем же самым проводам, которые используются для передачи и приема данных.

Когда вы подаете питание на устройства по тому же Ethernet кабелю, который подает данные, то все что вам нужно - это прикрепить сетевое PoE устройство к одному низковольтному Ethernet кабелю. Использование PoE устройств уменьшает необходимость протягивать электрические кабели и розетки к каждому месту, которое должно быть подключено к сети. Это не только значительно уменьшает стоимость установки сетевых устройств, это также увеличивает гибкость в смысле того, где эти устройства могут быть установлены и смонтированы. Перемещение устройств также проще, потому что все что требуется на новом месте - это Ethernet кабель с PoE питанием.

## Нестандартное PoE

Изначально продукты PoE были частными решениями, созданными отдельными компаниями, которые осознали необходимость технологии. Процесс IEEE по созданию стандарта PoE начался в 1999 году; однако, это заняло около четырех лет прежде, чем стандарт стал реальностью. И в это время, собственное PoE производителей продолжало производиться в больших количествах. Собственные решения PoE часто использовали разные напряжения, и смешивание частных решений могло привести к повреждению оборудования.

### IEEE 802.3af

Комитет *IEEE 802.3af Power over Ethernet* создал поправку PoE к стандарту 802.3. Официально это называлось IEEE 802.3 "Поправка: Питание Терминального Оборудования Передачи Данных (DTE) по Зависимому от Среды Интерфейсу" [IEEE 802.3 "Amendment: Data Terminal Equipment (DTE) Power via Media Dependent Interface"]. Эта поправка к стандарту IEEE 802.3, утвержденная 12 июня 2003 года, определяет как подать PoE к 10BaseT (Ethernet), 100BaseT (Fast Ethernet), и 1000BaseT (Gigabit Ethernet) устройствам.

### IEEE Std 802.3-2005, Статья 33

В Июне 2005 года IEEE пересмотрел стандарт 802.3, создав IEEE Std 802.3-2005. Поправка 802.3af была одной из четырех поправок, которые были включены в этот переработанный стандарт. В версии 2005 года стандарта 802.3 и в более свежих версиях (он был переработан в 2008, 2012, 2015, и еще раз в 2018 годах), Статья 33 - это раздел, который описывает PoE.

### IEEE 802.3at-2009

Поправка IEEE 802.3at былаratифицирована в 2009 году. *802.3at* также называется, как PoE+ или *PoE плюс*, так как она расширяет возможности PoE, изначально определенные в поправке 802.3 af. Две из основных целей Рабочей Группы 802.3at были сделать возможным подавать больше мощности запитываемым устройствам и поддерживать обратную совместимость с устройствами Статьи 33 (*Clause 33*). Так как ТД становятся быстрее и включают более новые технологии, они требуют больше мощности для работы. Коммутаторы и контроллеры, которые включают в себя технологию 802.3at, способны подать питание как устаревшим ТД, так и более новым ТД, которые требуют больше мощности. Устройства IEEE 802.3at способны обеспечить до 30 ватт мощности с использованием двух пар проводов в кабеле Ethernet. Поправка 802.3at определяет устройства с PoE как Тип1 [Type 1] или Тип 2 [Type 2]. Устройства, способные поддержать более высокую мощность, определенные в поправке 802.3at, определяются как устройства Тип 2, а устройства не способные поддерживать более высокую мощность, определяются как устройства Тип 1.

Обычно, когда создается и принимается поправка 802, документ поправки - это, фактически, серия дополнений, удалений и исправлений, который модифицируют и обновляют базовый стандарт. С 802.3at, раздел PoE (Статья 33) стандарта 802.3-2008 был целиком заменен поправкой 802.3at.

## IEEE Std 802.3-2018, Статья 33

В Декабре 2012 года, IEEE пересмотрел стандарт 802.3 снова и создал IEEE Std 802.3-2012. Также как поправка 802.3af включена в стандарт 802.3 в 2005 году, в выпуске 802.3-2012 переработанного стандарта поправка 802.3at была официально включено в эту новую версию. Стандарт снова был обновлен в 2015 году, а текущая версия это IEEE Std 802.3-2018.

## IEEE 802.3bt-2018

Поправка 802.3bt была третьей итерацией PoE и описывается в новой статье – 145.

Введено два дополнительных типа оборудования подачи питания [power-sourcing equipment (PSE)] и питаемых устройств [powered device (PD)] - 3 и 4. Хотя были введены новые мощностные возможности, устройства 802.3bt обратно совместимы с устаревшими устройствами Типа 1 и Типа 2. В дополнение к увеличению числа типов PoE, были добавлены четыре новых класса мощности, с 5-ого по 8-ой, дополняя предыдущие классы с 0-ого по 4-ый.

Четыре новых уровня мощности обеспечиваются блоками питания. Эти уровни – это 45 Вт, 60 Вт, 75 Вт, и 90 Вт. 802.3bt подает питание по всем четырем парам проводов и включает поддержку устройств 10GBase-T.

Таблица 12.1 предоставляет обзор поправок и технических характеристик каждого из девяти классов мощности.

**ТАБЛИЦА 12.1** Обзор PoE

IEEE Стандарт	Год Принятия	Класс	Мощности	Тип PoE	# Пар Ethernet	Мощн ость PSE	Мощн ость PD
802.3af	2005	0	15.4	1	2	15.4 Вт	12.95 Вт
802.3af	2005	1	30	1	2	4 Вт	3.84 Вт
802.3af	2005	2	45	1	2	7 Вт	6.49 Вт
802.3af	2005	3	60	1	2	15.4 Вт	12.95 Вт
802.3at	2009	4	75	2	2	30 Вт	25.5 Вт
802.3bt	2018	5	90	3	4	45 Вт	40 Вт
802.3bt	2018	6	105	3	4	60 Вт	51 Вт
802.3bt	2018	7	120	4	4	75 Вт	62 Вт
802.3bt	2018	8	135	4	4	90 Вт	71.3 Вт

# Устройства с PoE

Стандарт PoE определяет два типа устройств с PoE: потребители или питаемые устройства [powered device (PD)] и оборудование подачи питания [power-sourcing equipment (PSE)]. Эти устройства общаются друг с другом и обеспечивают инфраструктуру PoE. До 802.3bt, устройства с PoE использовали две пары кабеля Ethernet для подачи питания. С принятием 802.3bt, PoE может теперь также предоставляться по всем четырем парам кабеля Ethernet. Способ и число пар Ethernet, используемых для подачи питания от оборудования подачи питания [PSE] к потребителю [PD] согласовывается при начальном подключении устройства.

## Питаемые Устройства

*Питаемое устройство [powered device (PD)]* или запрашивает, или получает питание от оборудования подачи питания. Если PD не поддерживает 802.3bt, то оно должно уметь принимать до 57 вольт от или линий с данными, или по неиспользуемым парам кабеля Ethernet. PD должен также быть способен принимать питание с полярностью от блока питания в , что называется, режиме А или режиме В, как описано в Таблице 12.2.

**ТАБЛИЦА 12.2** Распиновка Питаемого Устройства (PD)

Проводник в кабеле Ethernet	Режим А	Режим В
1	Положительное напряжение, отрицательное напряжение	
2	Положительное напряжение, отрицательное напряжение	
3	Отрицательное напряжение, положительное напряжение	
4		Положительное напряжение, отрицательное напряжение
5		Положительное напряжение, отрицательное напряжение
6	Отрицательное напряжение, положительное напряжение	
7		Отрицательное напряжение, положительное напряжение
8		Отрицательное напряжение, положительное напряжение

PD должен ответить оборудованию подачи питания *сигнатурой обнаружения [detection signature]* и уведомить PSE находится ли оно в состоянии, в котором оно готово принять питание или не готово принять питание. Сигнатура обнаружения также используется для индикации, что PD совместима с оригинальным стандартом PoE. Если устройство определено как несовместимое, питание на устройство не будет подано.

Если устройство находится в состоянии, в котором оно будет принимать питание, PD может опционально предоставить *классификационную сигнатуру [classification signature]* оборудованию подачи питания [PSE]. Эта классификационная сигнатура позволяет оборудованию подачи питания узнать сколько мощности понадобится устройству.

Устройства Типа 2, которые были введены с 802.3af, выполняют двух событийную классификацию Физического уровня или классификацию Канального [Data-Link] уровня, которые позволяют PD Типа 2 идентифицировать подключено ли оно к PSE типа 1 или Типа 2. Если взаимная идентификация не может быть выполнена, то устройство может работать только как устройство Типа 1. Эта техника двух событийной классификации была расширена на Тип 3 и Тип 4 устройств PSE и PD, которые поддерживают 802.3bt.

Таблица 12.3 перечисляет список значений токов, используемых для идентификации различных классификационных сигнатур. Если ни одно из этих значений токов не измерено, то считается что устройство будет устройством Класса 0. Если устройство не идентифицировано, то PSE не знает сколько мощности нужно устройству; следовательно, оно занимает максимальную мощность. Если устройство классифицировано, то PSE занимает только количество мощности, необходимое PD, таким образом обеспечивая лучшее управление питанием. Соответствующая классификация устройств может привести к управляемому снижению в используемой мощности и может также позволить вам подключить больше устройств к одному PoE коммутатору.

**ТАБЛИЦА 12.3** Величины измеряемых электрических токов классификационных сигнатур PD

Параметр	Условия	Минимум	Максимум
Класс 0	14.5 В to 20.5 В	0 миллиампер (mA)	4 mA
Класс 1	14.5 В to 20.5 В	9 mA	12 mA
Класс 2	14.5 В to 20.5 В	17 mA	20 mA
Класс 3	14.5 В to 20.5 В	26 mA	30 mA
Класс 4	14.5 В to 20.5 В	36 mA	44 mA

В прошлом, некоторые производители использовали собственные протоколы обнаружения 2 уровня, чтобы выполнить классификацию. Хотя эти методы хороши с точки зрения управления питанием и потребления, но они являются проприетарными и не будут работать с продуктами других производителей. Протокол Обнаружения Канального Уровня [Link Layer Discovery Protocol (LLDP)] является протоколом обнаружения соседей на 2ом уровне на основе стандартов, и который также может быть использован для более детальной мощностной классификации. Таблица 12.4 перечисляет классы устройств PoE и диапазон максимальной мощности, который они используют. Классы от 0 до 3 для устройств Типа 1, которые будут работать с оборудованием подачи питания 802.3af. Класс 4 предназначен для устройств Типа 2, которые работают с оборудованием подачи питания 802.3at (PoE+). Классы с 5 по 8 для устройств Типа 3 и Типа 4, которые работают с 802.3bt.

Максимальная подаваемая мощность 12,95 ватт для 802.3af-совместимого устройства, 25,5 ватт для 802.3at-совместимого устройства, и 71,3 ватта для 802.3bt-совместимого устройства.

**TABLE 12.4** Классификация Питания PD и Использование

Класс	Использование	Диапазон Максимальной Используемой Мощности	Стандарт PoE
0	По умолчанию	от 0,44 Вт до 12,95 Вт	802.3af
1	Опционально	от 0,44 Вт до 3,84 Вт	802.3af
2	Опционально	от 3,84 Вт до 6,49 Вт	802.3af
3	Опционально	от 6,49 Вт до 12,95 Вт	802.3af
4	Устройства Типа 2	от 12,95 Вт до 25,5 Вт	802.3at
5	Устройства Типа 3	от 25,5 Вт до 40 Вт	802.3bt
6	Устройства Типа 3	от 40 Вт до 51 Вт	802.3bt
7	Устройства Типа 4	от 51 Вт до 62 Вт	802.3bt
8	Устройства Типа 4	от 62 Вт до 71,3 Вт	802.3bt

#### Какой категории кабель мне следует использовать для ТД, питаемой по PoE ?

Стандарт PoE имеет ограничение по длине кабеля Ethernet в 100 метров (328 футов) для передачи данных и подачи питания, и для IEEE 802.3af (PoE) и для 802.3at (PoE+).

Стандарты PoE требуют кабель категории 5 (CAT 5) чтобы удовлетворять ограничениям по длине. Производители БЛВС рекомендуют использовать кабели категории 5е (CAT5e) или лучше, чтобы удовлетворять и требованиям PoE и требованиям полосы 1Гиг (1000 Мбит/с). Так как ТД требуют большую полосу восходящего канала, то необходима категория 6а (CAT 6a) или кабель более высокого класса, чтобы поддержать 10 000 Мбит/с.

## Оборудование Подачи Питания

*Оборудование подачи питания [power-sourcing equipment (PSE)]* подает питание к PD. Питание подается с номиналом в 48 вольт (от 48 вольт до 57 вольт). PSE ищет питаемые устройства с помощью детектирующего сигнала постоянного тока. После того, как PoE-совместимое устройство идентифицировано, PSE подает питание к этому устройству. Если устройство не отвечает на сигнатуру обнаружения [detection signature], PSE не подает питание. Это предотвращает от повреждения несовместимое питаемое оборудование (PD).

Как вы можете видеть в Таблице 12.5, количество мощности, подаваемое PSE, больше, чем то что используется PD (Таблица 12.4). Это потому, что PSE нужно рассчитывать на худший сценарий, в котором могут быть потери мощности на кабеле и разъемах между PSE и PD.

Максимальная подача любому питаемому устройству – 71,3 ватта. PSE может также классифицировать PD, если PD предоставляет классификационную сигнатуру. Подключившись, PSE непрерывно проверяет состояние соединения PD вместе с мониторингом других электрических условий, таких как короткое замыкание. Когда питание больше не требуется, PSE останавливает его подачу. Оборудование подачи питания поделено на два типа оборудования: конечное [endpoint] и промежуточное [midspan].

**ТАБЛИЦА 12.5** Мощность PSE

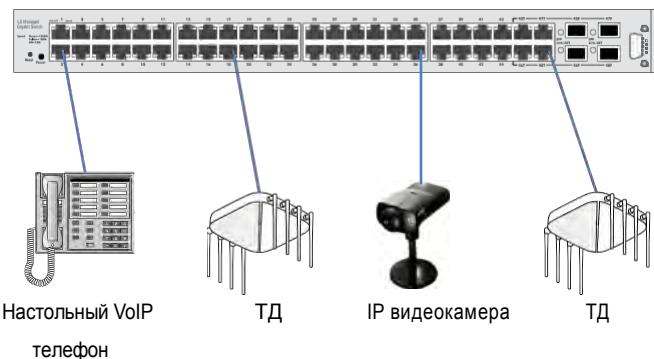
Класс	Минимальная Мощность от Pse	Стандарт
0	15,4 Вт	802.3af
1	4,0 Вт	802.3af
2	7,0 Вт	802.3af
3	15,4 Вт	802.3af
4	30,0 Вт	802.3at
5	45,0 Вт	802.3bt
6	60,0 Вт	802.3bt
7	75,0 Вт	802.3bt
8	90,0 Вт	802.3bt

## Конечное оборудование подачи питания

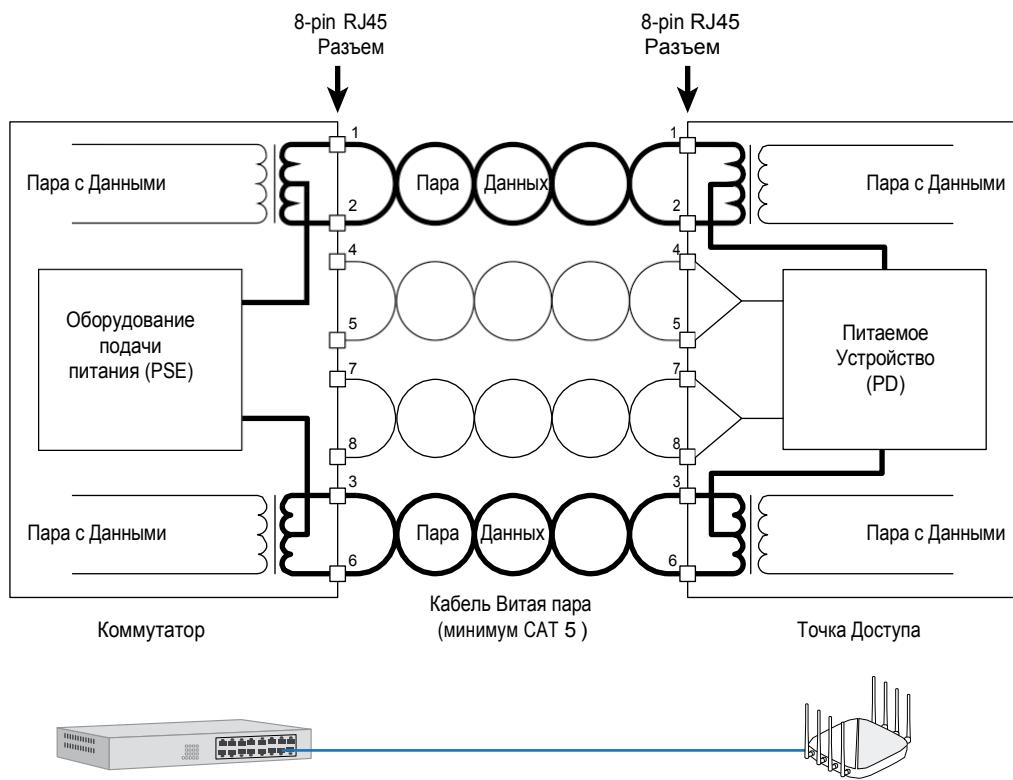
*Конечное оборудование подачи питания* [endpoint PSE] подает и питание и сигналы данных Ethernet от одного и того же устройства. Конечные устройства – это обычно Ethernet коммутаторы с PoE, такие как 48 портовый коммутатор, показанный на Рисунке 12.1. PoE-коммутаторы используются для подачи питания устройствам уровня доступа (таким как ТД и телефоны), а следовательно коммутаторы являются коммутаторами уровня доступа, а не коммутаторами распределения или ядра. Некоторые специальные устройства, такие как контроллеры БЛВС, БЛВС маршрутизаторы филиалов, или настенные ТД с PoE портом также могут работать как конечное оборудование подачи питания [endpoint PSE equipment]. Большинство ТД, управляемых контроллером, запитываются коммутатором уровня доступа; однако, некоторые небольшие модели или контроллеры БЛВС филиалов могут также быть использованы, чтобы запитать точки доступа.

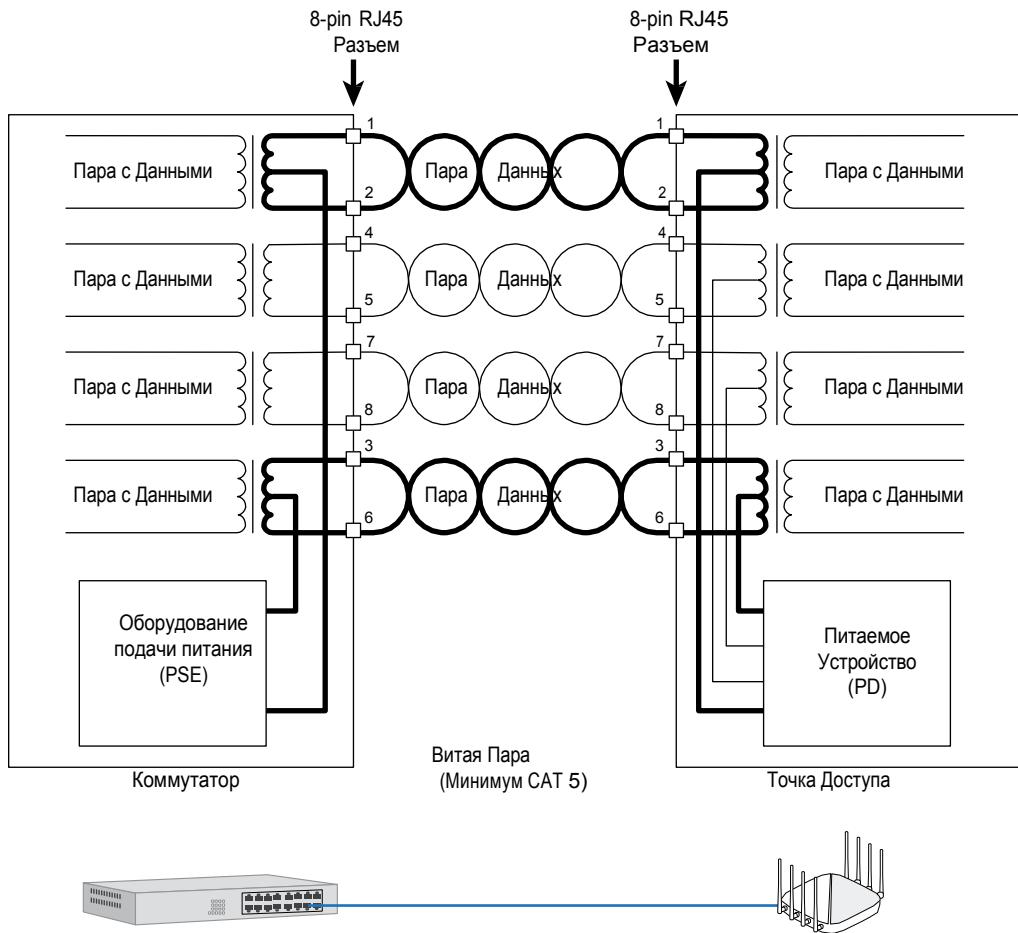
## Конечное оборудование подачи питания по 2м парам

Конечное оборудование, использующее две пары Ethernet проводов, может подавать питание с использованием двух способов, называемых Альтернатива А [Alternative A] и Альтернатива В [Alternative B].

**РИСУНОК 12.1** 48-портовый Gigabit Ethernet коммутатор доступа с PoE

**Альтернатива А** В Альтернативе A [Alternative A], PSE подает питание по паре для передачи данных. Рисунок 12.2 показывает как конечное оборудование подачи питания [PSE] 10BaseT/100BaseTX подает питание, используя Альтернативу А, и Рисунок 12.3 показывает как конечное PSE 1000/2.5G/5G/10GBaseT подает питание, используя Альтернативу А.

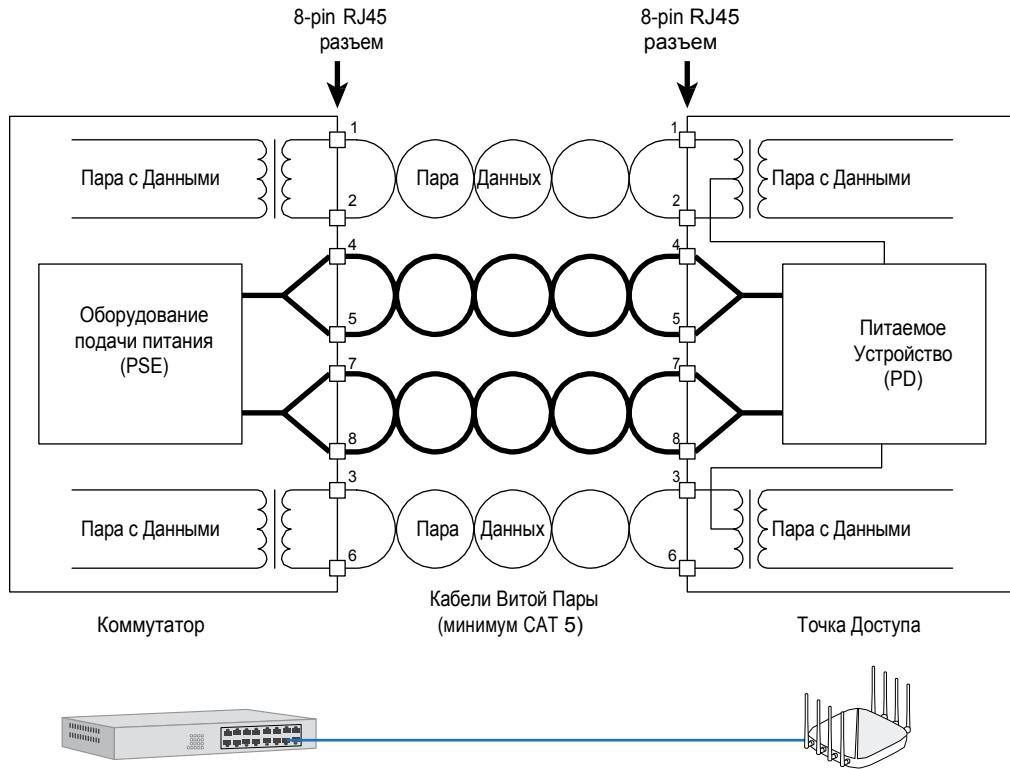
**РИСУНОК 12.2** Конечное 2x парное 10BaseT/100BaseTX PSE, Альтернатива А

**FIGURE 12.3** Конечное 2x парное 1000/2.5G/5G/10GBaseT PSE, Альтернатива A

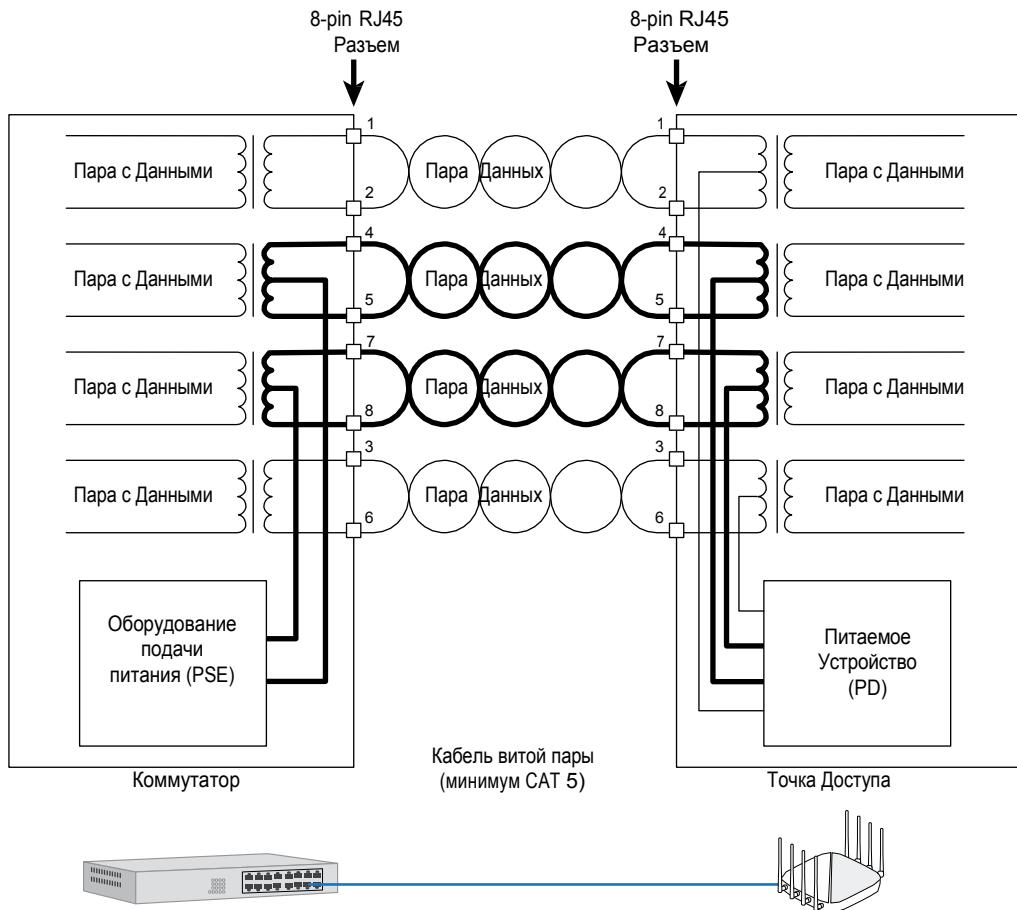
**Альтернатива В** Изначально, Альтернатива B [Alternative B] была создана для подачи питания по отдельным неиспользуемым парам проводов в кабеле 10BaseT/100BaseTX, как показано на Рисунке 12.4. Конечное PSE 1000BaseT также может использовать Альтернативу B для подачи питания к PD, подавая питание на две пары с данными 1000BaseT, как показано на Рисунке 12.5. Конечное PSE совместимо с 10BaseT (Ethernet), 100BaseTX (Fast Ethernet), и 1000BaseT (Gigabit Ethernet).

Когда 802.3af был впервыеratифицирован, устройства 1000BaseT (Gigabit Ethernet) могли получать PoE только от конечных устройств. В следующем разделе этой главы вы увидите, что это больше не верно. С принятием 802.3at, устройства 1000BaseT могут также получать питание, используя или конечное PoE или промежуточное PoE. Ратификация 802.3bt еще больше расширила поддержку для устройств 1000/2.5G/5G/10GBaseT, используя четыре пары Ethernet.

**РИСУНОК 12.4** 2x парное конечное PSE 10BaseT/100BaseTX, Альтернатива B



**РИСУНОК 12.5** 2x парное конечное PSE 1000/2.5G/5G/10GBaseT, Альтернатива В



**Конечное оборудование подачи питания по 4 парам.**

802.3bt-совместимое конечное оборудование с PoE может использовать четыре пары Ethernet для подачи питания конечным устройствам 10BaseT/100BaseTX, как показано на Рисунке 12.6, или конечным точкам 1000/2.5G/5G/10GBaseT, как показано на Рисунке 12.7.

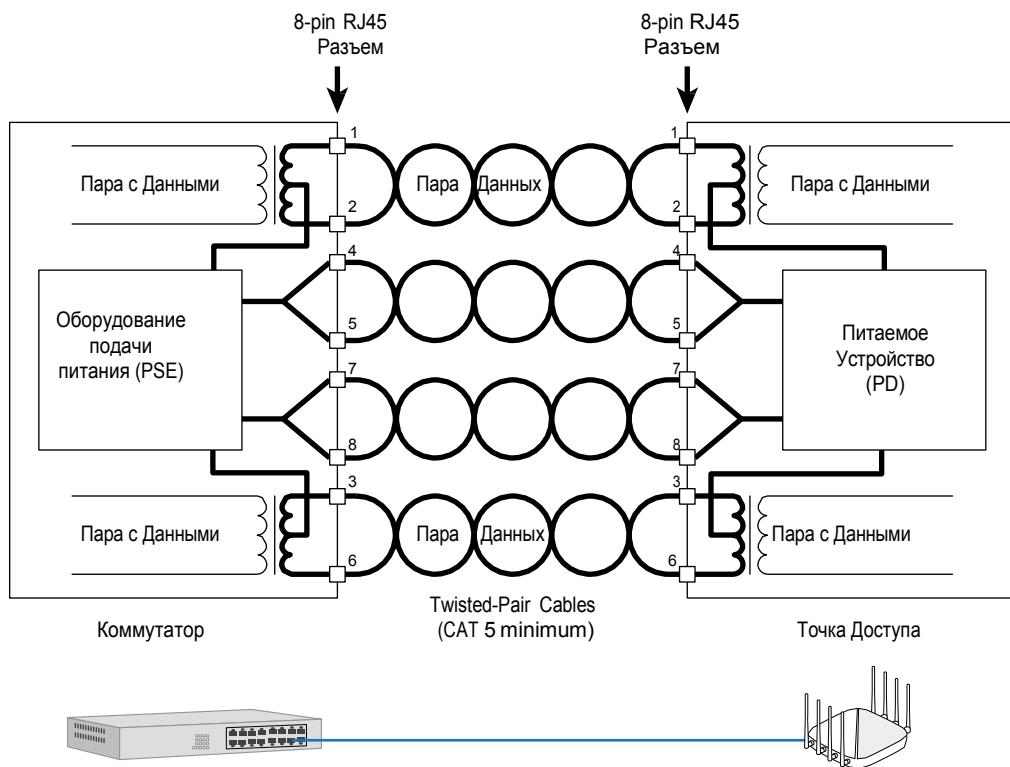
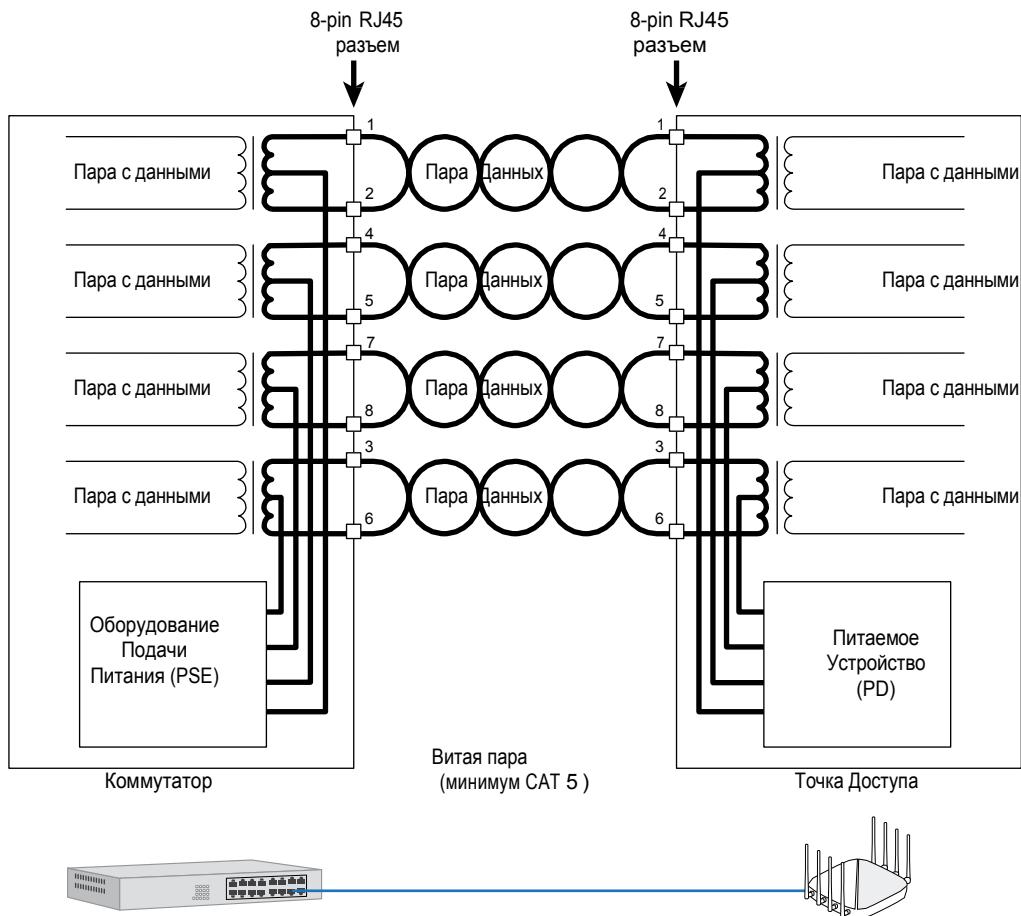
**РИСУНОК 12.6** 4x парное конечное PSE 10BaseT/100BaseTX

РИСУНОК 12.7 4x парное конечное PSE 1000/2.5G/5G/10GBaseT



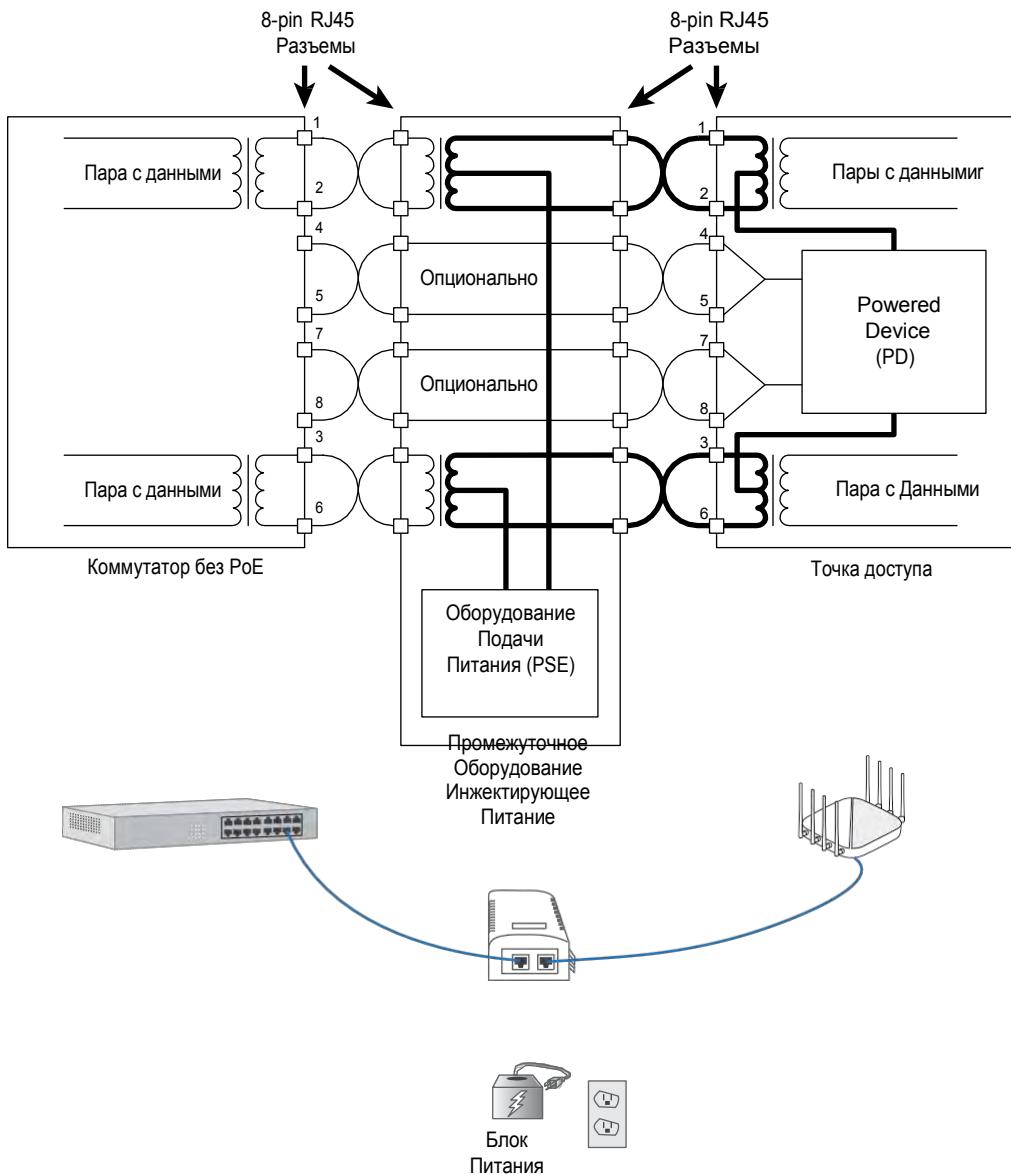
## Промежуточное оборудование подачи питания

*Промежуточное оборудование подачи питания [midspan PSE]* действует как сквозное устройство, добавляющее питание в Ethernet сегмент. Промежуточное оборудование позволяет подать PoE в существующие сети без необходимости замены существующих коммутаторов Ethernet. Промежуточное PSE размещается между источником Ethernet (такими как Ethernet коммутатор) и потребителем [PD]. Промежуточное PSE действует как повторитель [repeater] Ethernet, добавляя питание к Ethernet кабелю. Изначально, в 802.3af, промежуточные устройства были способны использовать только Альтернативу B - и только с питаемыми устройствами [PD] с 10BaseT и 100BaseTX. С принятием 802.3at, промежуточные устройства стали способны использовать или Альтернативу A или Альтернативу B, и могли обеспечить поддержку устройства 1000BaseT. С ратификацией 802.3bt промежуточные устройства могут подавать питание, используя или две пары или четыре пары проводов к питаемым устройствам [PDs] 10BaseT/100Base-TX или 1000Base-T/2.5G/5G/10GBaseT.

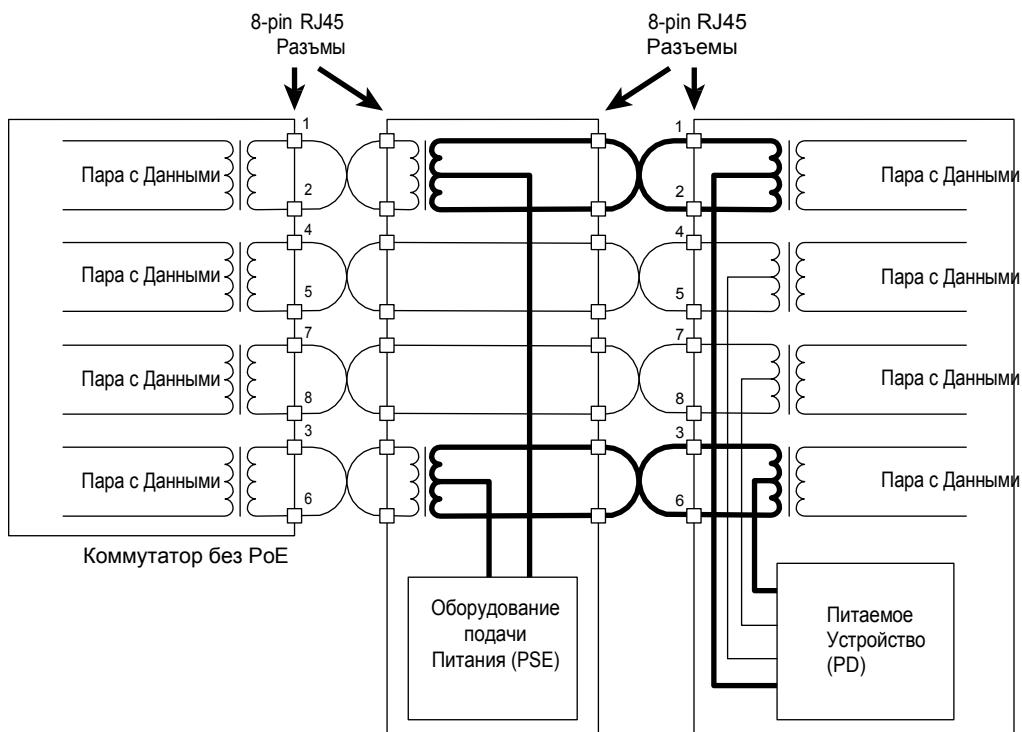
## Промежуточное оборудование подачи питания по 2м парам

Рисунок 12.8 показывает как промежуточное PSE 10BaseT/100BaseTX подает питание, используя Альтернативу A, и Рисунок 12.9 показывает, как промежуточное PSE 1000BaseT/2.5G/5G/10GBaseT подает питание с использованием Альтернативы A. Рисунок 12.10 показывает промежуточное PSE 10BaseT/100BaseTX, подающее питание с использованием Альтернативы B, и Рисунок 12.11 показывает, как промежуточное PSE 1000BaseT подает питание с использованием Альтернативы B.

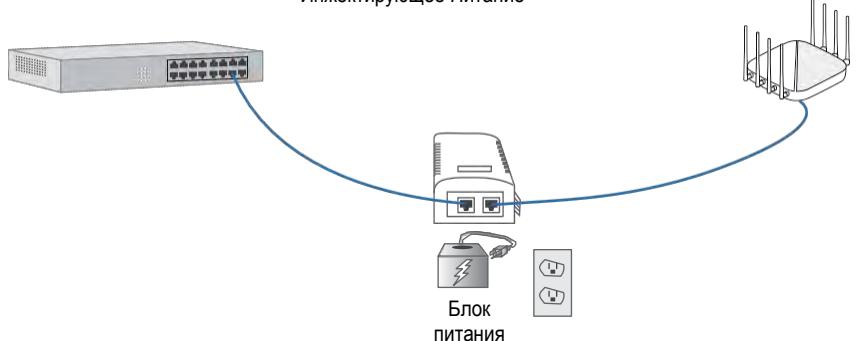
**РИСУНОК 12.8** 2x парное промежуточное PSE 10BaseT/100BaseTX, Альтернатива A



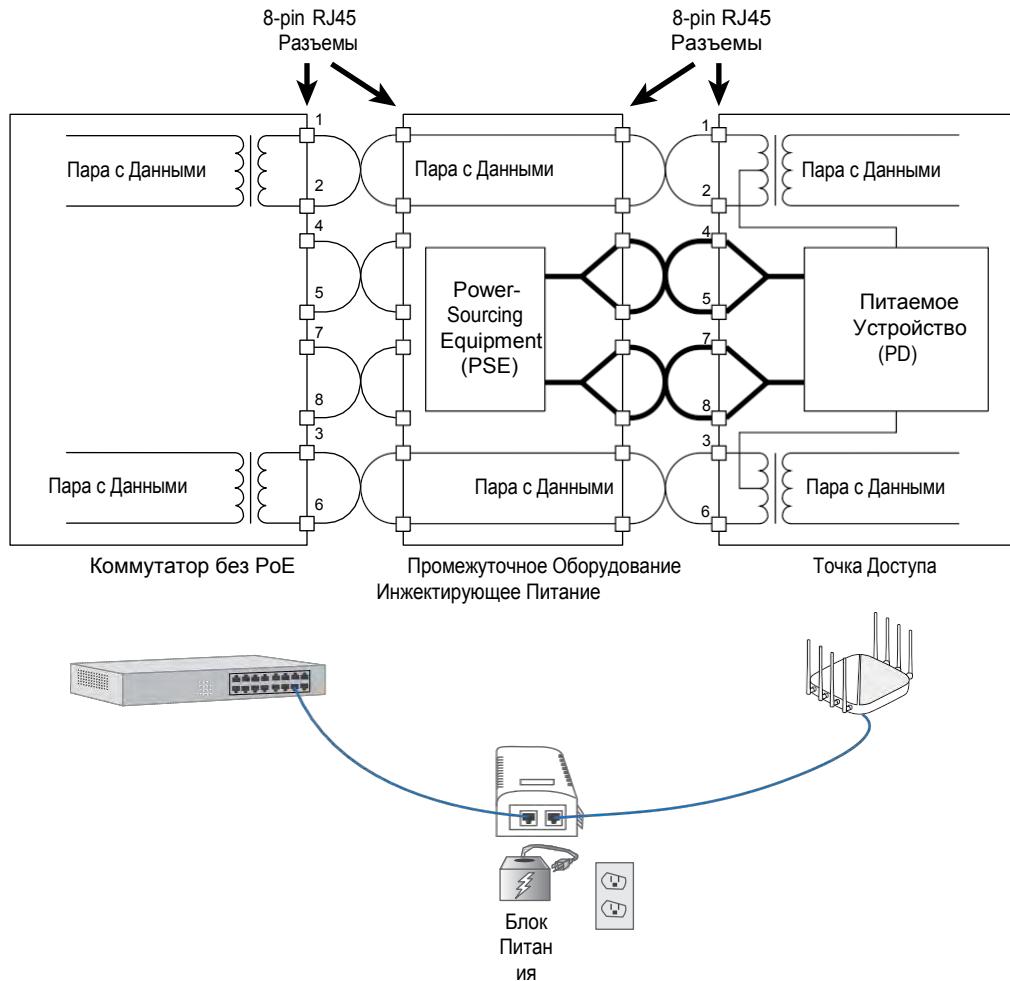
**РИСУНОК 12.9** 2x парное промежуточное PSE 1000BaseT/2.5G/5G/10GBaseT, Альтернатива A



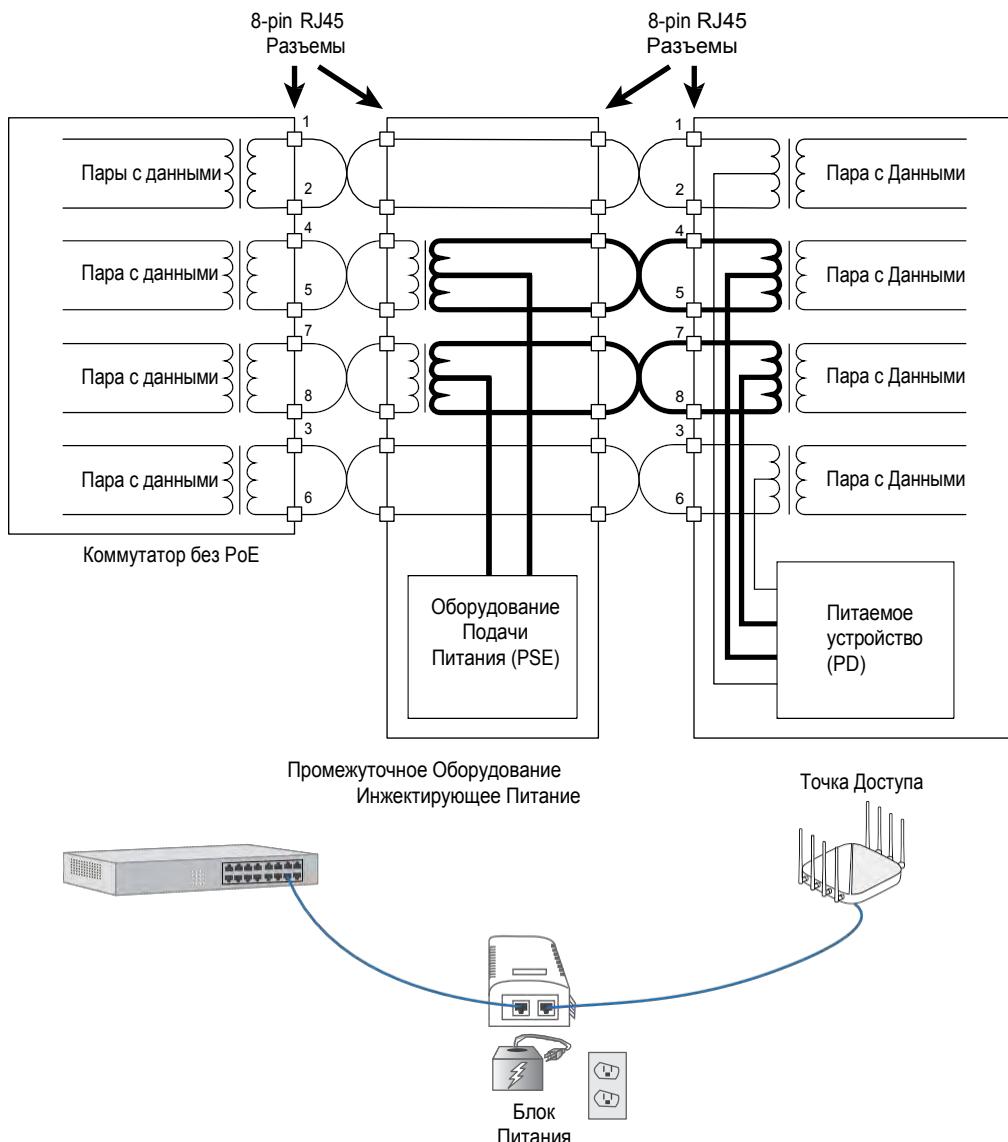
Промежуточное Оборудование  
Инжектирующее Питание



**РИСУНОК 12.10** 2x парное промежуточное PSE 10BaseT/100BaseTX, Альтернатива В



**РИСУНОК 12.11** 2x парное промежуточное PSE 1000BaseT/2.5G/5G/10GBaseT, Альтернатива B



## Промежуточное оборудование подачи питания по 4-м парам.

Рисунок 12.12 показывает как 10BaseT/100BaseTX промежуточное оборудование подачи питания по 4-м парам [4-pair midspan PSE] подает питание питаемому [PD], и Рисунок 12.13 показывает как 4x парное промежуточное PSE 1000BaseT/2.5G/5G/10GBaseT подает питание потребителю [PD].

**РИСУНОК 12.12** 4x парное промежуточное PSE 10BaseT/100BaseTX

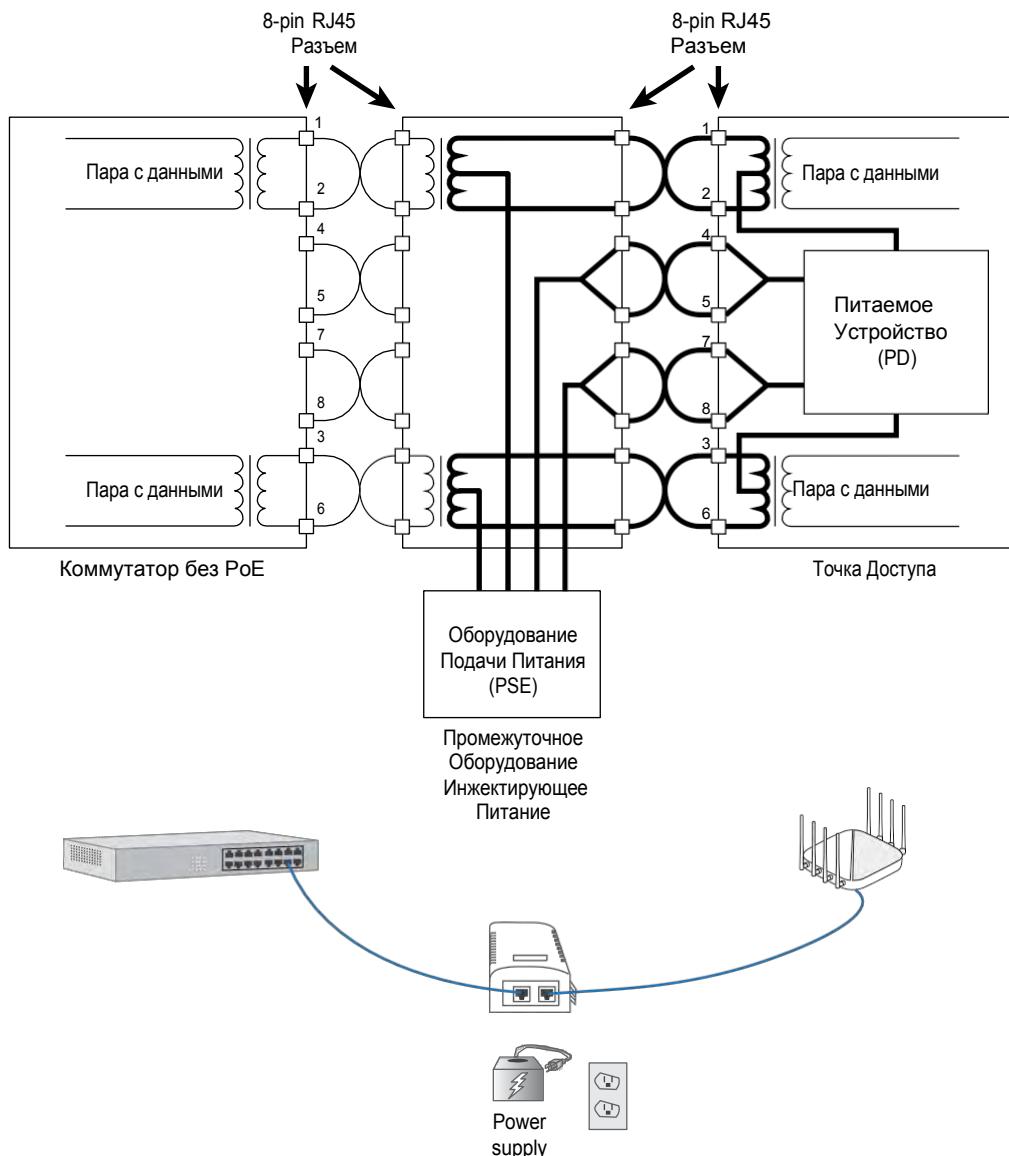
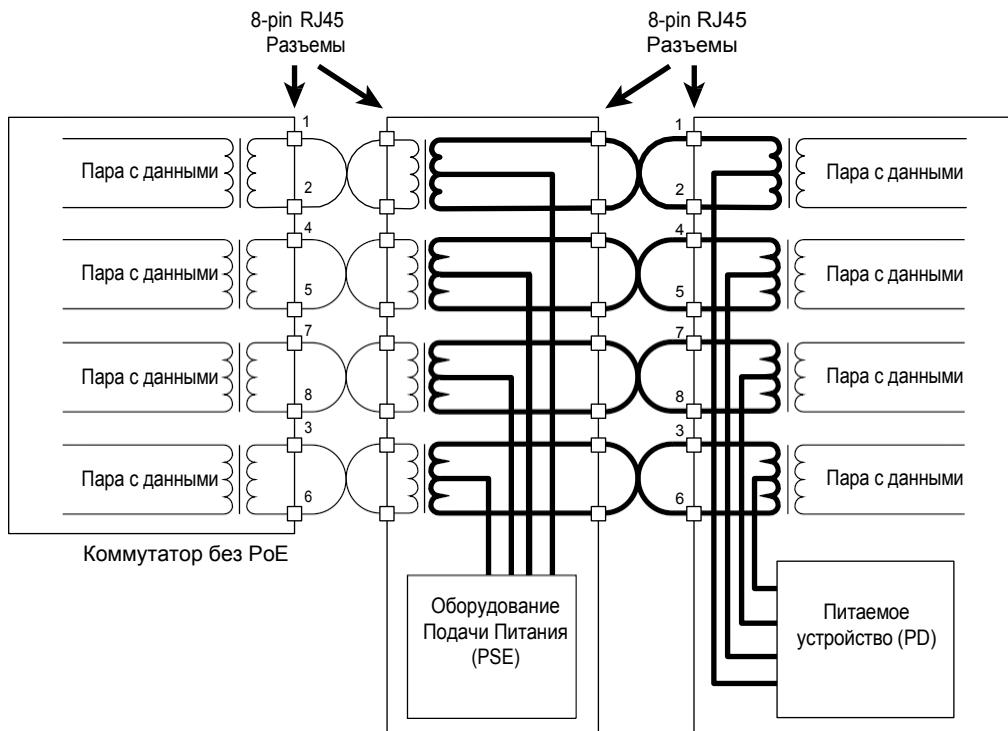


РИСУНОК 12.13 4x парное промежуточное PSE 1000BaseT/2.5G/5G/10GBaseT

Промежуточное Оборудование  
Инжектирующее Питание

Точка Доступа



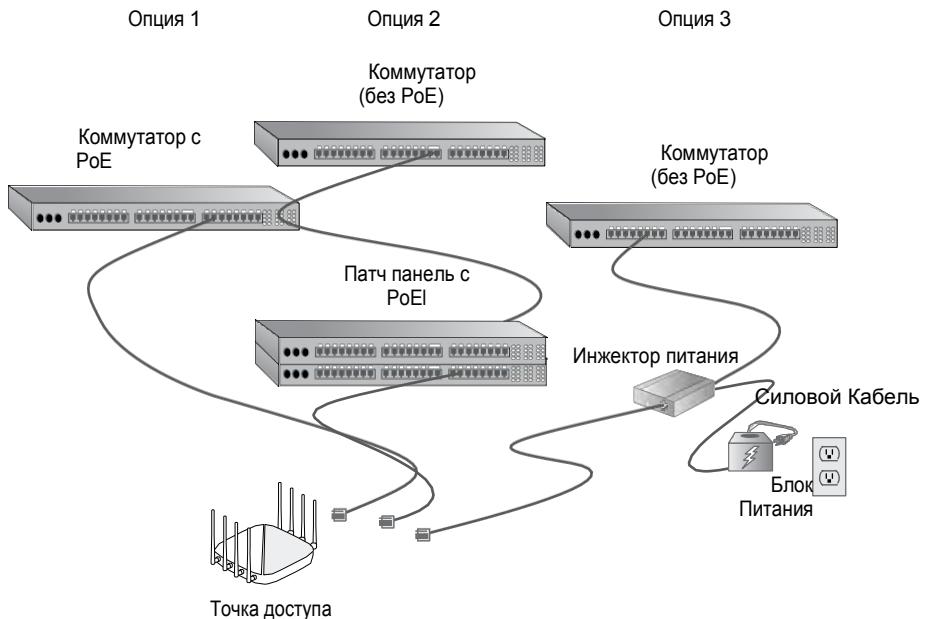
Рисунок 12.14 показывает однопортовое промежуточное устройство вместе с тремя многопортовыми устройствами. Промежуточное оборудование подачи питания [midspan PSE] обычно называют инжектором питания [power injector] (однопортовое устройство) или PoE Хаб [PoE hub] (многопортовое устройство).

**РИСУНОК 12.14** Инжектор питания PowerDsine и PoE хабы.



Рисунок 12.15 показывает три типовых способа подачи питания питаемому устройству [PD]. Опция 1 иллюстрирует конечный коммутатор с PoE с питанием в линии связи. Этот коммутатор предоставляет и Ethernet и питание для ТД. Опция 2 и Опция 3 иллюстрируют два способа промежуточной подачи питания. Опция 2 показывает многопортовое промежуточное PSE, обычно называемой как *патч-панель с PoE [inline power patch panel]*, и Опция 3 показывает однопортовое оборудование подачи питания [*midspan PSE*], обычно называемое *однопортовый инжектор питания [single-port power injector]*.

**РИСУНОК 12.15** Три решения оборудования подачи питания



# Планирование и Развёртывание PoE

В прошлом, когда настольные VoIP телефоны без PoE и ТД без PoE были подключены к сети, у каждого устройства была своя индивидуальная электрическая розетка. Эти розетки были распределены по всему зданию или кампусу, распределяя потребности по питанию. PoE консолидирует источник питания всех PoE устройств в коммутационном шкафу или датацентре (центре обработки данных), требуя, чтобы только Ethernet кабель был подключен к устройству с питанием по PoE.

## Планирование Мощности

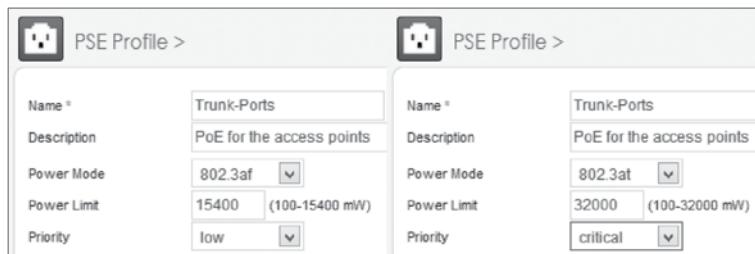
Вместо того, чтобы распределять мощность по сотням или тысячам устройств, мощность для этих устройств теперь подается из одного или ограниченного количества мест. При максимальной мощности для PD, PSE должно быть способно подать до 90 Вт мощности каждому PoE устройству. Если ваши PD требуют PoE+, это значит, что типовой 24-портовый коммутатор Ethernet с PoE должен уметь обеспечить около 612 ватт мощности, чтобы подать на 24 порта ( $25,5 \text{ ватт} \times 24 \text{ порта} = 612 \text{ ватт}$ ). Это не включает количество мощности, необходимой коммутатору для осуществления сетевых операций. Простой способ вычисления достаточно ли мощный блок питания коммутатора - это определить размер блока питания для аналогичного коммутатора без PoE и добавить необходимые ватты для каждого PoE устройства, которое будет подключено к коммутатору.

Так как много устройств, таких как ТД 802.11, видео камеры, настольные VoIP телефоны могут требовать питание, может возникать ситуации, когда просто не достаточно доступных ватт, чтобы запитать все PoE порты. Сетевые инженеры стали осознавать необходимость *бюджетов мощности [power budget]*. Тщательное планирование нужно, чтобы гарантировать, что достаточно мощности доступно для всех питаемых устройств [PDs]. Питаемые устройства, которые поддерживают классификацию, могут значительно помочь в сбережении энергии и вычитанию меньшего количества мощности из бюджета мощности. Устройства, которым нужно подавать 3 ватта, но они не способны предоставить классификационную сигнатуру, будут классифицированы как Класс 0 по умолчанию, и вычтут 15,4 ватта из общего бюджета мощности. Фактически, 12 ватт мощности будет простиавать в пустую. Если то же самое устройство было бы способно поддержать классификационную сигнатуру, и было бы классифицировано как устройство Класса 1, то только 4 ватта было бы вычтено из общего бюджета мощности. Классификация питаемых устройств [PD] будет расти по значимости по мере роста необходимости в развертывании БЛВС.

Производители коммутаторов уровня предприятия приводят бюджет мощности PoE на листе спецификации коммутатора. Бюджет мощности PoE, приведенный в листке спецификации, является действительным количеством мощности, которое доступно на портах и не предназначено для других функций коммутатора. При чтении спецификации бюджета мощности, удостоверьтесь сколько портов поддерживает PoE. Например, у Производителя А может быть 24x-портовый гигабитный коммутатор с бюджетом мощности PoE в 195 ватт, но бюджет доступен только на 8 из 24 портов. Производитель В может также предложить 24x-портовый гигабитный коммутатор с бюджетом мощности PoE в 195 ватт, но бюджет может быть доступен на любом из 24 портов. Производитель С может продать 24x-портовый коммутатор с много большим бюджетом мощности PoE в 408 ватт, доступных всем 24 портам. Держите в уме, что чем больше бюджет мощности, тем больше растет стоимость PoE-коммутатора.

Как показано на Рисунке 12.16, у большинства коммутаторов есть возможность определить возможности порта. Точки доступа 802.11 могут быть нужны все 25,5 ватт, подаваемые 802.3at портом; однако, настольному VoIP телефону может быть нужно только 7 ватт от порта. Порт 802.3af для телефона может быть вручную настроен только для 7 ватт, и следовательно, сберечь 8,4вата, которые не нужно будет вычитать из общего бюджета мощности PoE. Порты PoE часто могут также быть настроены с уровнем приоритета. PoE порты с более высоким приоритетом имеют преимущество в получении питания в случае, когда PoE бюджет исчерпан. Правильное планирование PoE бюджета гарантирующее, что бюджет никогда не будет исчерпан, - является лучшей практикой. Приоритет порта PoE также важен, если есть неисправность оборудования коммутатора. У коммутаторов PoE часто есть несколько блоков питания. Если один из блоков питания ломается, то коммутатор не сможет обеспечить мощность всем подключенным к нему устройствам. Приоритет порта PoE позволяет сетевому администратору определить какие устройства являются более критичными, чем другие.

**РИСУНОК 12.16** Бюджетирование PoE на уровне портов



Следует наблюдать за бюджетом мощности коммутатора или нескольких коммутаторов, чтобы убедиться, что все устройства могут получать питание. Активную информацию о бюджете PSE можно обычно посмотреть в командной строке коммутатора или в графическом интерфейсе [GUI], или отслеживать централизованным сервером управления сетью [*network management server (NMS)*]. В примере, показанном на Рисунке 12.17, общий бюджет коммутатора 195 ватт. Точка доступа включена в порт 1 и на текущий момент использует 7,4 ватта, в тоже время другая ТД, включенная в порт 2, на текущий момент потребляет 3 ватта. Общая мощность используемая на текущий момент составляет 10,4 ватта, что означает, что 184,6 ватт могут использоваться другими устройствами. В этом примере, одна из ТД классифицирована как устройство класса 0, что означает, что оно может потреблять до 12,95 ватт. Если ТД не очень занята, ей может быть нужно только 3 или 5 ватт, но если на ТД много подключенных клиентов с тяжелым трафиком, могут понадобится все 12,95 ватт.

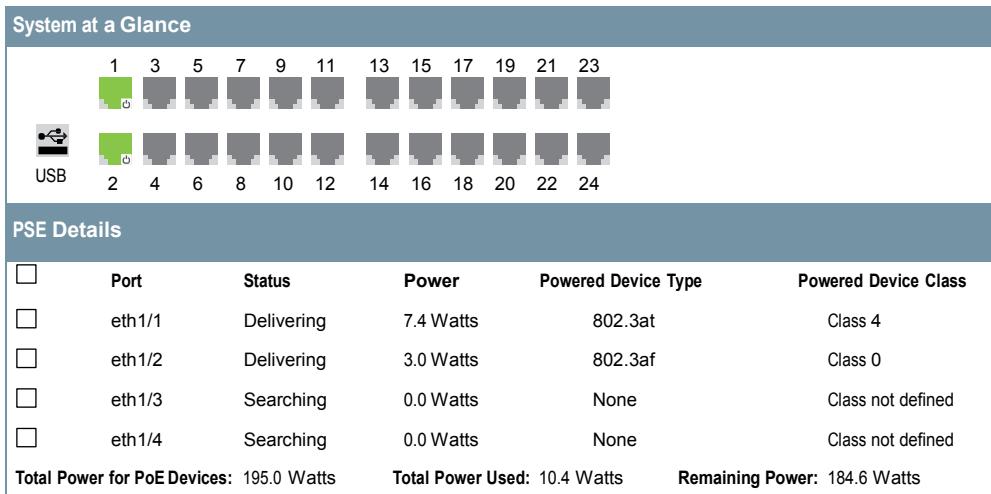
Следовательно, всегда планируйте ваш бюджет мощности на основе максимального потребления, которое устройство, такие как точки доступа, могут использовать.

#### Почему мои точки доступа хаотично перезапускаются ?

Производители БЛВС обычно получают звонки на тех.поддержку от заказчиков, жалующихся, что все их точки доступа внезапно стали хаотически перезагружаться. Во многих случаях, причиной случайного перезапуска ТД в том, что бюджет мощности коммутатора уменьшился. Очень часто, если ТД не может получить мощность, которая ей нужна, то ТД перезапускается и пытается снова. Помните, что другие устройства,

такие как настольные VoIP телефоны, также используют PoE. Такое дополнительное устройство с PoE может быть включено в порт коммутатора и бюджет мощности будет превышен. Соответствующее бюджетирование мощности для точек доступа и любых других устройств с PoE является первостепенным. Неисправные кабели или кабели, которые превышают 100 метров, могут также привести к недостатку мощности или непостоянной мощности, и стать причиной перезагрузки ТД.

**РИСУНОК 12.17** Мониторинг бюджета мощности



Из-за увеличения спроса на устройства с PoE, некоторые производители коммутаторов заменили свой блоки питания 110 вольт/30 ампер на блоки питания 220 вольт/20 ампер. Производители также помещают еще большие блоки питания в свои коммутаторы, чтобы справляться с дополнительными требованиями PoE. Некоторые коммутаторы с PoE обеспечивают до 9000 ватт. По мере роста запроса на PoE устройства, необходимость в управлении и поиска проблем PoE также растет. Тестеры, такие как показанный на Рисунке 12.18, могут быть установлены между PSE и PD, чтобы найти проблему на линии с PoE.

Чем больше устройств с PoE вы добавляете к сети, тем больше концентрируете требования к питанию в центре обработки данных или коммутационном шкафу. По мере роста ваших потребностей по питанию, может потребоваться увеличение электрических цепей, подающие питание коммутаторам с PoE. Также, при росте мощности, количество генерируемого тепла в коммутационных шкафах растет, что часто требует большего количества оборудования для контроля климата. Когда вы используете высоковаттные блоки питания, мы рекомендуем, чтобы вы также использовали резервные блоки питания.

**РИСУНОК 12.18** Сетевой тестер NetAlly LinkSprinter



## Резервирование

Детьми, мы знали, что даже когда пропадало электричество, телефон продолжал работать и давал возможность позвонить кому-нибудь. Это является тем уровнем сервиса, который мы ожидаем получить. Телефоны VoIP и VoWiFi заменяют традиционные телефонные системы, и важно продолжать обеспечивать тот же уровень непрерывного сервиса. Чтобы достичь этого, вам нужно убедиться, что все ваше оборудование подачи питания по PoE подключено к источникам бесперебойного питания. Дополнительно, может быть достаточно важным обеспечить двойное Ethernet соединение с вашим питаемым оборудованием по PoE.

Некоторые ТД производителей БЛВС предлагают два Ethernet PoE порта с возможностями незаметного переключения в целях резервирования PoE. ТД могут быть подключены проводами к двум отдельным коммутаторам с PoE, которые установлены в двух разных кабельных стойках промежуточного распределительного узла.

### Будьте осторожны с PoE

С ростом популярности PoE и требованием к подаче питания устройствам, таким как ТД и VoIP телефоны, устанавливается больше розеток PoE в офисном пространстве. Одна приятная и необходимая характеристика PoE в том, что когда устройство подключено, PSE может определить является ли устройство с PoE, и если так, то подать питание на это устройство. Если устройство без PoE, то Ethernet будет без подачи питания на это устройство.

В зависимости от бренда и модели вашего коммутатора с PoE, когда PoE-устройство отсоединяется от коммутатора, для порта на коммутаторе возможна поддержка PoE состояния еще несколько секунд, даже когда ничего не включено в коммутатор. Если вы быстро подключите другое устройство в этот же порт, то возможно, что коммутатор с PoE

подаст питание на это устройство, даже если оно является устройством без PoE. Это представляет риск повреждения устройства.

Чтобы предотвратить возникновение такого риска, после отсоединения любого Ethernet устройства, вам следует взять за привычку ждать 5-10 секунд, прежде чем подключать другое устройство в тот же порт или розетку. Эта задержка в 5-10 секунд должна быть достаточно долгой, чтобы порт PoE деактивировался. Затем, когда другое устройство подключится в этот порт, PoE будет определять поддерживает ли новое устройство PoE.

## Понижение возможностей PoE

К сожалению, иногда ТД может быть подключена к Ethernet порту с PoE, который не способен подать ТД требуемую мощность. Это может происходить из-за того, что ТД включена в порт, который обеспечивает старое, менее мощное PoE, например: ТД 4×4:4 включена в PoE порт 802.3af, вместо порта PoE 802.3at. Еще один сценарий, когда это может случиться – это когда ТД включена в коммутатор, который не способен поддерживать все PoE устройства, включенные в него, или возможно, что один из блоков питания в коммутаторе стал неисправен, уменьшив количество мощности, доступной PoE portам.

Многие производители БЛВС уровня предприятия включают в свои ТД технологию для работы с этой проблемой. Один способ – это уменьшить возможности MIMO точки доступа. Поскольку связь на 5ГГц обычно более важная, чем связь на 2,4ГГц, уменьшение числа радиоцепей в радиомодуле 2,4ГГц до 1×1:1 является одним методом уменьшения требований ТД к мощности. Производитель также может уменьшить число радио цепей в радиомодуле 5ГГц. Если у ТД есть несколько Ethernet портов, еще один способ сбережения мощности – это отключение всех дополнительных Ethernet портов, оставляя активным только Ethernet порт для подключения к сети [uplink]. Другие сетевые интерфейсы, такие как радиомодуль Bluetooth с низким энергопотреблением [Bluetooth Low Energy (BLE)], могут также быть отключены для уменьшения потребляемой мощности.

В конечном счете, важно планировать вашу сеть с соответствующими возможностями PoE так, чтобы ваши устройства получали необходимую мощность, позволяя им работать с их оптимальными характеристиками, так чтобы сеть работала в соответствии с тем как она спроектирована.

## Доводы по мощности 802.3bt

Как вы уже знаете, 802.3bt определяет четыре новые уровня мощности 45 Вт, 60 Вт, 75 Вт, и 90 Вт, подаваемые оборудованием подачи питания. Коммутаторы с 802.3bt уровня предприятия сейчас продаются на рынке. Поэтому вопрос: нужна ли вам мощность 45 Вт или выше на порту коммутатора чтобы в достаточной мере запитать точку доступа? Большинство точек доступа уровня предприятия являются двухдиапазонными ТД в форм факторах 4×4:4, 3×3:3, или 2×2:2.

15,4 ватта (802.3af) являются достаточными, чтобы запитать все компоненты  $2\times2:2$  и  $3\times3:3$  двух диапазонных ТД. Однако, двух диапазонные точки доступа  $4\times4:4$  обычно требуют 30 Вт (802.3at). Некоторые производители БЛВС продают ТД  $8\times8:8$ , и требования по мощности PoE для них еще более солидны.

С появлением 802.11ax, некоторые производители БЛВС производят премиальные ТД с радиомодулем  $8\times8:8$  (5 ГГц) и радиомодулем  $4\times4:4$  (2,4 ГГц). В некоторых случаях, эти ТД  $8\times8:8$  будут требовать 31 ватт или больше, что означает, что даже питания PoE плюс будет недостаточно. В то же время некоторые ТД  $8\times8:8$  могут быть питаны от 802.11at (PoE Плюс), так как существует своего рода понижение по функциональности, такого как отключение USB, радиомодуля BLE и т.д.

В большинстве случаев, мощность 802.3bt не нужна для запитывания современных точек доступа. Однако, помните, что PoE это не только ТД. Многие другие устройства, которые требуют намного большей мощности, становятся широко распространенными. Например, камеры видеонаблюдения с функциями панорамирования [pan], наклона [tilt] и масштабирования [zoom] обычно требуют 30-60 Вт. Многочисленные типы промышленного оборудования требуют больше 30 Вт. Медицинские системы вызова медсестры часто требуют 50 Вт. Большое количество установок корпоративных коммутаторов будут требовать 802.3bt, чтобы запитать эти устройства, в то время как мощность 802.3at или меньше останется достаточной для запитывания точек доступа.

Итак, будет ли необходимость в мощности 802.3bt в будущем, чтобы запитывать БЛВС? Как ранее отмечалось, очень небольшое количество премиальных ТД  $8\times8:8$  может требовать мощность 802.3bt. Однако, с полосой частот 6ГГц на горизонте, производители Wi-Fi будут производить ТД с еще большим количеством радиоцепей. Например, премиальная ТД может иметь четыре радиомодуля: радиомодуль  $8\times8:8$  (6 ГГц), радиомодуль  $4\times4:4$  (5 ГГц), радиомодуль  $4\times4:4$  (2,4 ГГц), и сенсорный радиомодуль  $2\times2:2$ . Потребность в мощности 802.3bt 45 Вт будет необходима, когда вы объедините эти радиомодули Wi-Fi с радиомодулями BLE, радиомодулями UWB, и USB портами.

Большинство производителей будут пытаться спроектировать ТД, которые по прежнему могут запитывать мощностью 802.3at: радиомодуль  $4\times4:4$  (6 ГГц), радиомодуль  $4\times4:4$  (5 ГГц), и радиомодуль  $2\times2:2$  (2,4 ГГц). В зависимости от форм фактора ТД и числа радиоцепей, некоторым будущим поколениям ТД вероятно будет нужна мощность 802.3bt.

## Пучки Кабеля 802.3bt

Когда коммутаторы 802.3bt станут более распространенными, потребуется принимать во внимание особые меры предосторожности при складывании в пучки кабелей, которые используют питание Типа 4 в 90 Вт. Когда используется PoE Тип 4, по кабелям течет до 960 миллиампер (mA) по каждой паре.

Спецификация кабеля определяет  $45^\circ$  С ( $113^\circ$  F) как максимальную базовую температуру окружающей среды. Если не указано иное,  $+15^\circ$  С выше базовой температуры окружающей среды ( $60^\circ$  С) считается абсолютным максимумом для температурного класса CAT 5e/CAT 6/CAT 6a. Все что больше  $15^\circ$  С над базовой температурой считается слишком горячим и потенциально опасным.

Когда кабели, подающие питание PoE Тип 4, свяжены вместе, очень легко превысить  $15^\circ$  С над базовой температурой окружающей среды. Максимальный размер пучка, разрешенный для  $15^\circ$  градусного повышения от температуры окружающей среды в  $45^\circ$  С, показан в Таблице 12.6. Затененные области таблицы показывают потенциально опасные размеры пучков кабелей при использовании PoE Типа 4.

**ТАБЛИЦА 12.6** Повышение температуры в пучках кабеля

Число Кабелей в Пучке	Повышение Температуры на Пару (°C)					
	Category 5e	Category 6	Category 6A	Category 5e	Category 6	Category 6A
Воздух	Кабельканал	Воздух	Кабельканал	Воздух	Кабельканал	Кабельканал
1	1.1	1.7	0.8	1.3	0.7	1.1
7	3.5	5.2	2.6	4.0	2.3	3.3
19	6.7	9.7	5.1	7.4	4.4	6.1
37	10.7	15.2	8.2	11.6	7.0	9.5
61	15.5	21.6	12.0	16.6	10.1	13.4
91	21.0	29.0	16.4	22.2	13.8	17.9
127	27.3	37.4	21.4	28.6	17.9	23.0
169	34.4	46.6	27.1	35.7	22.6	28.6

Обратите внимание, что если 61 кабель САТ 5е связаны вместе на открытом воздухе, то температура повышается выше приемлемого уровня в 15° С над базовой температурой окружающей среды. Если используется кабель канал, то уже 37 кабелей превосходят приемлемый уровень.

Нижняя линия это, если PoE устройства, которые требуют 90Вт мощности станут широко распространенными, то тщательное рассмотрение должно быть проведено при объединении кабелей в пучки, чтобы избежать любой возможной опасности возгорания. Заметьте, что кабели категорий САТ 7 и САТ 8 имеют более высокие температурные классы, но эти категории кабелей не широко используются на предприятиях.

## ИТОГО

Эта глава концентрируется на Питании по Ethernet [Power over Ethernet] и оборудовании и методах необходимых для предоставления сервиса питаемым устройствам [PD]. Питание по Ethernet [Power over Ethernet] может быть подано двумя основными способами: по проприетарному PoE или по стандартному PoE (802.3af или 802.3at, включенные в IEEE Std 802.3 в Статью 33; или 802.3bt).

Стандартный PoE состоит из нескольких ключевых компонентов:

- Питаемое устройство [Powered Device (PD)]
- Оборудование подачи питания [Power-sourcing equipment (PSE)]

- Конечное оборудование подачи питания [Endpoint PSE]
- Промежуточное оборудование подачи питания [Midspan PSE]
  - Эти компоненты работают вместе, чтобы обеспечить функционирование PoE среды.
  - Финальный раздел этой главы охватывает доводы, которые нужно будет сделать при планировании и развертывании PoE:
- Планирование мощности
- Резервирование

## Темы Экзамена

**Знать историю PoE.** Убедитесь, что вы знаете историю PoE, исходную поправку 802.3af, поправку 802.3at, текущую ссылку на стандарт IEEE Std 802.3, Статья 33, вместе с поправкой 802.3bt

**Быть знакомым с различными устройствами PoE, и как они совместно работают.** Убедитесь, что вы знаете о различных устройствах PoE и их роли в обеспечении PoE. Понимать как следующие устройства работают: питаемое устройство [powered device (PD)], оборудование подачи питания [power-sourcing equipment (PSE)], конечное оборудование подачи питания [endpoint PSE], и промежуточное оборудование подачи питания [midspan PSE].

**Знать различные классы устройств и процесс классификации.** Убедитесь, что вы знаете пять классов устройств и как работает процесс классификации для определения класса PD. Знать какой ток каждого класса устройств используется вместе с тем сколько мощности генерирует PSE для каждого класса устройств.

## Контрольные Вопросы

1. Поправки IEEE 802.3af и 802.3at были включены в переработанный стандарт IEEE Std 802.3-2018 и определены в какой статье?
  - A. Статья [Clause] 15
  - B. Статья [Clause] 17
  - C. Статья [Clause] 19
  - D. Статья [Clause] 33
  - E. Статья [Clause] 43
2. Если не предоставлена классификационная сигнатурा, то считается, что устройство какого класса?
  - A. 0
  - B. 1
  - C. 2
  - D. 3
  - E. 4
3. Какой тип устройств PoE определен стандартом? (Выберите все, что применимо.)
  - A. PSE
  - B. PPE
  - C. PD
  - D. PT
4. Питаемое устройство [powered device (PD)] должно быть способно получать до скольких вольт по проводам с данными и неиспользуемым парам кабеля Ethernet?
  - A. 14,5 вольт
  - B. 20,5 вольт
  - C. 48 вольт
  - D. 57 вольт
5. Чтобы квалифицировать как совместимое с поправкой 802.3at (теперь часть стандарта 802.3), что из перечисленного должно делать питаемое устройство (PD)? (Выберите все, что применимо.)
  - A. Быть способным получать питание по неиспользуемым парам
  - B. Отвечать PSE сигнатурой обнаружения [detection signature]
  - C. Получать питание любой полярности от PSE
  - D. Ответить PSE классификационной сигнатурой [classification signature]
6. Телефон VoIP подключен к 24 портовому промежуточному оборудованию подачи питания [midspan PSE] PoE. Если телефон не предоставляет классификационную сигнатуру, то сколько мощности подаст PSE телефону?
  - A. 12,95 ватта
  - B. 4,0 ватта

- C.** 7,0 ватт  
**D.** 15,4 ватта
- 7.** Какая поправка представила поддержку PoE по четырем парами Ethernet?  
**A.** 802.3af  
**B.** 802.3at  
**C.** 802.3bt  
**D.** 802.11 статья 33  
**E.** Все PoE используют две пары Ethernet
- 8.** Какой максимальный диапазон мощности используется PD Класса 4?  
**A.** 0,44–12,95 ватта  
**B.** 3,84–6,49 ватта  
**C.** 6,49–12,95 ватта  
**D.** 12,95–25,5 ватта  
**E.** 15–30 ватт
- 9.** В максимальных требованиях по мощности, 24-портовый 802.3at-совместимый Ethernet коммутатор PoE сколько всего ватт должен быть способен обеспечить PoE устройствам на всех портах?  
**A.** 15,4 ватта  
**B.** 370 ватт  
**C.** 720 ватт  
**D.** 1000 ватт  
**E.** Предоставлено не достаточно информации для ответа на вопрос.
- 10.** Если 802.3bt-совместимая ТД оснащена двумя радиомодулями и требует 35 ватт по питанию, сколько мощности подаст ей PSE?  
**A.** 35 ватт  
**B.** 40 ватт  
**C.** 45 ватт  
**D.** 60 ватт  
**E.** 90 ватт
- 11.** PSE подает питание в диапазоне \_\_\_\_\_ вольт, с номинальным значением \_\_\_\_\_ вольт.  
**A.** 14,5–20,5; 18  
**B.** 6,49–12,95; 10,1  
**C.** 12–19; 15,4  
**D.** 44–57; 48

- 12.** Джон установил коммутатор Ethernet, который совместим с 802.3at. У него есть проблемы с хаотически перезагружающимися ТД. Что из следующего может быть причиной его проблем?
- A.** Много PoE VoIP телефонов подключены к тому же самому Ethernet коммутатору.
  - B.** Большинство Ethernet кабелей идущих от коммутатора к ТД являются 90 метровыми.
  - C.** Ethernet кабели только CAT 5e.
  - D.** Коммутатор поддерживает 1000BaseT, который не совместим с VoIP телефонами.
- 13.** Анна проектирует 802.3at-совместимую сеть и устанавливает 24 портовый Ethernet коммутатор для поддержки 10 VoIP телефонов Класса 1 и 10 ТД класса 0. Коммутатор требует 500 ватт для работы его базовых функций по коммутации. Сколько всего мощности будет нужно?
- A.** 500 ватт
  - B.** 694 ватта
  - C.** 808 ватт
  - D.** 1 000 ватт
- 14.** Джордж проектирует сеть с поддержкой 802.3at и устанавливает 24 портовый Ethernet коммутатор для поддержки 10 камер Класса 2 и 10 ТД Класса 3. Коммутатор требует 1000 ватт для выполнения своих базовых функций по коммутации. Сколько всего мощности будет нужно?
- A.** 1080 ватт
  - B.** 1224 ватта
  - C.** 1308 ватт
  - D.** 1500 ватт
- 15.** Когда установлена сеть с PoE, каково максимальное расстояние от PSE до PD, согласно стандарта? (Выберите все, что применимо.)
- A.** 90 метров
  - B.** 100 метров
  - C.** 300 футов
  - D.** 328 футов
  - E.** 328 метров
- 16.** Какова максимальная потребляемая мощность 802.3bt PD?
- A.** 12,95 ватта
  - B.** 15 ватт
  - C.** 60 ватт
  - D.** 51 ватт
  - E.** 90 ватт
  - F.** 71,3 ватта

- 17.** Какая максимальная мощность используется устройством PD Класса 0?
- A.** 3,84 ватта
  - B.** 6,49 ватта
  - C.** 12,95 ватта
  - D.** 15,4 ватта
- 18.** PSE подает напряжение между 14,5 и 20,5, и измеряет результирующий ток, чтобы определить класс устройства. Какой диапазон токов представляет устройства Класса 2?
- A.** 0–4 mA
  - B.** 5–8 mA
  - C.** 9–12 mA
  - D.** 13–16 mA
  - E.** 17–20 mA
- 19.** PD должен быть способен принимать питание с любой полярностью от блока питания. Используя Альтернативу A, по каким проводникам/проводам PD принимает питание?
- A.** 1, 2, 3, 4
  - B.** 5, 6, 7, 8
  - C.** 1, 2, 3, 6
  - D.** 4, 5, 7, 8
- 20.** PSE Типа 4 будет выполнять двух событийную классификацию на Физическом уровне или классификацию на Канальном уровне. Если взаимная идентификация не может быть выполнена, что делает устройство Типа 4?
- A.** По умолчанию это устройство Категории 0.
  - B.** Оно работает как устройство Типа 2.
  - C.** Оно работает как устройство Типа 1.
  - D.** Он подает 15,5 ватт питания, используя Альтернативу A.



# Глава 13



## Концепции Проектирования БЛВС

---

**В ЭТОЙ ГЛАВЕ ВЫ УЗНАЕТЕ О СЛЕДУЮЩЕМ:**

✓ **Планирование покрытия БЛВС**

- Принятый сигнал
- Отношение сигнал-шум
- Динамическое переключение скоростей
- Мощность передачи

✓ **Планирование Роуминга**

- Первичное и вторичное покрытие
- Быстрый безопасный роуминг
- Роуминг Уровня 3

✓ **Планирование каналов**

- Интерференция смежных каналов
- Переиспользование каналов 2,4ГГц
- Одноканальная интерференция
- Переиспользование каналов 5 ГГц
- Каналы DFS
- Проектирование каналов 40МГц
- Статические каналы и мощность передачи или адаптивное радио
- Одноканальная архитектура

✓ **Планирование емкости**

- Высокая плотность
- Управление выбором полосы
- Балансировка нагрузки
- Потребление эфирного времени



- ✓ Голос или данные
- ✓ Два 5 ГГц и программно-определенное радио
- ✓ Проектирование 6ГГц БЛВС
  - Обзор клиентов
  - Обзор покрытия
  - Переиспользование 6 ГГц каналов
  - Обнаружение ТД 6 ГГц
  - Безопасность Wi-Fi в 6 ГГц
- ✓ Физическая среда
- ✓ Антенны
- ✓ Наружное проектирование



Если вы соберете 300 Wi-Fi экспертов в одной комнате, например как на конференции Профессионалов БЛВС [WLAN Professionals conference] ([www.wlanpros.com](http://www.wlanpros.com)), скорее всего вы получите 300 разных мнений как правильно проектировать БЛВС для покрытия, емкости и использования эфирного времени.

Опытные профессионалы БЛВС согласятся с важностью правильно спроектированной БЛВС. Основной вал звонков по устраниению проблем может быть предотвращен, если БЛВС хорошо спланирована и спроектирована до развертывания. Столь же важным является послеустановочное контрольное радио обследование для подтверждения дизайна/проекта БЛВС. Слабо спроектированная БЛВС без соответствующего подтверждения часто ведет к ненужному поиску и устранению проблем и дополнительным операционным расходам. Эта глава обсуждает концепции проектирования БЛВС, которые каждому администратору беспроводных сетей следует уверенно знать. Несмотря на то, что планирование БЛВС для обеспечения надлежащего покрытия имеет решающее значение, это всего лишь один из аспектов проектирования БЛВС. Хороший дизайн БЛВС должен также принимать во внимание емкость пользователей и устройств, чтобы обеспечить потребности в производительности. Из-за полудуплексной природы радиосреды, ключевая цель в проекте БЛВС - это уменьшить потребление эфирного времени [airtime]. В действительности, подход шаблонного проектирования/дизайна никогда не работает, потому что у разных вертикальных рынков разные потребности. Более того, каждое здание имеет уникальную планировку и, следовательно, разные свойства распространения и затухания радиоволн.

Эта глава обсуждает аспекты проектирования покрытия, емкости и интеграции БЛВС с концептуальной точки зрения. Однако, профессионалы БЛВС не всегда согласны относительно проекта/дизайна БЛВС, и у каждого может быть свой собственный уникальный подход. Независимо от того какой проектный подход вы используете, всегда помните о важности послеустановочного контрольного радио обследования [post-installation validation survey].

## Проектирование покрытия БЛВС

Когда вы проектируете БЛВС, вероятно, первое, что приходит на ум - это область покрытия или зона, из которой Wi-Fi клиенты могут работать. Цели первичного покрытия для любой БЛВС - это обеспечить высокоскоростное соединение для подключенных клиентов и обеспечить бесшовный роуминг. Распространенная типовая ошибка - это проектировать БЛВС только на основе характеристик точек доступа. На этапе проектирования следует рассматривать совершенно обратное. Правильный дизайн покрытия БЛВС должен опираться на точку зрения Wi-Fi клиентов. То есть, качественный принятый сигнал для клиента является необходимым для обеспечения соединения с высокой скоростью передачи данных и хорошего пользовательского опыта.

## Принятый Сигнал

Итак, что точно считается качественным принятым сигналом? Как показано в Таблице 13.1, в зависимости от близости между ТД и Wi-Fi клиентом, радиомодуль 802.11 может принимать входящие сигналы где-то между –30дБм и уровнем шума. При проектировании покрытия, обычный рекомендуемый лучший подход - это обеспечить –70 дБм или более сильный принятый сигнал, который заметно выше уровня шума. Другими словами, принятый сигнал в –70дБм и выше считается качественным принятым сигналом. При проектировании соединений с высокой скоростью передачи данных, сигнал –70 дБм или сильнее является требуемым.

**ТАБЛИЦА 13.1** Сила Принятого Сигнала

Качество	дБм	мВт
Очень Сильный	–30 дБм	1/1000-ая от 1милливатта
Очень Сильный	–40 дБм	1/10 000-ая от 1 милливатта
Очень Сильный	–50 дБм	1/100 000-ая от 1 милливатта
Очень Сильный	–60 дБм	1 миллионная от 1 милливатта
Сильный	–70 дБм	1 десятимиллионная от 1 милливатта
Нормальный	–80 дБм	1 стомиллионная от 1 милливатта
Слабый	–90 дБм	1 миллиардная от 1 милливатта
Очень Слабый	–95 дБм	Уровень шума

Следует понимать, что не все клиентские устройства созданы одинаковыми. Например, максимальная скорость передачи данных, возможная для устаревших клиентов 802.11g, это 54 Мбит/с, в то время как радиомодуль 802.11n/ac 2×2:2 МIMO может поддерживать скорость передачи данных 300 Мбит/с. Более того, в зависимости от производителя чипсета, радиомодули различных клиентов Wi-Fi имеют разные пороги приемной чувствительности, которые соответствуют разным скоростям передачи данных. Это значит, что два клиентских радиомодуля, принимающих радиосигнал с одной и той же силой, могут использовать разные скорости передачи данных для модуляции и демодуляции. Несмотря на различия между устройствами и чувствительностью, общий знаменатель все же есть. Принятый сигнал в –70 дБм и выше обычно гарантирует, что клиентский радиомодуль будет использовать одну из высоких скоростей передачи данных, на которую способен клиент. При проектировании БЛВС для передачи голоса, рекомендуемым является –65 дБм или более сильный принятый сигнал. Держите в голове, что фактическая зона действия сигнала –65 дБм будет меньше, чем сигнала –70 дБм. Рисунок 13.1 изображает зону покрытия –70 дБм в сравнении с зоной покрытия ячейки – 65 дБм.

**РИСУНОК 13.1** Покрытие  $-70$  дБм и  $-65$  дБм

В Главе 14 "Радиообследование и Контрольная проверка" вы узнаете об инструментах предиктивного моделирования, которые могут помочь вам при планировании зон покрытия  $-70$  дБм или  $-65$  дБм для отдельных ТД. Еще раз, запомните, что действительная зона покрытия ТД определяется с точки зрения Wi-Fi клиента, и подтверждение любого планируемого покрытия является необходимостью. Так как чувствительность индикатора силы принятого сигнала [received signal strength indicator] (RSSI) различаются между устройствами БЛВС, контрольное радиообследование часто выполняется с использованием различных типов Wi-Fi клиентов.

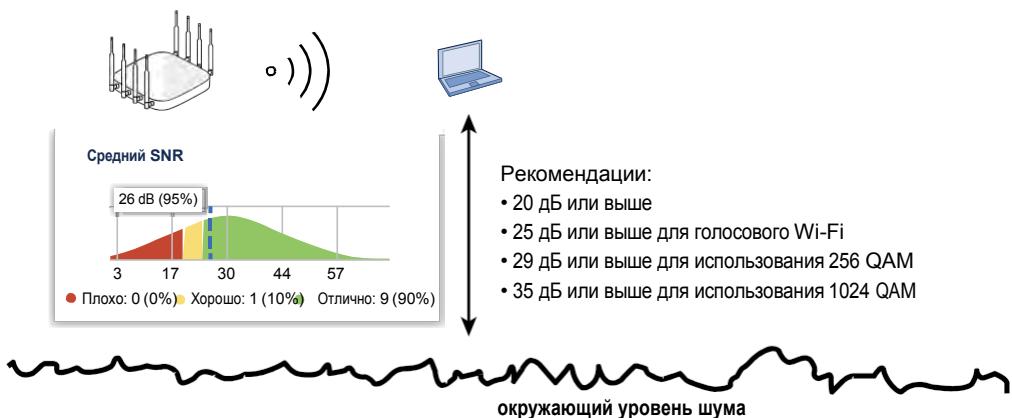
## Отношение Сигнал-Шум

Еще одной причиной для планирования покрытия для  $-70$  дБм в том, что принятый сигнал в  $-70$  дБм обычно достаточно высок над уровнем шума. В Главе 4 "Радио Компоненты, Измерения и Математика" вы узнали, что *отношение сигнал-шум* [*signal-to-noise ratio (SNR)*] является важным значением, потому что, если фоновый шум слишком близок к принятому сигналу или уровень принятого сигнала слишком низкий, данные могут быть повреждены. SNR это не реальное отношение; это просто разница в децибелах между принятым сигналом и фоновым шумом (уровнем шума), измеренная в дБ, как показано на Рисунке 13.2. Если радиомодуль 802.11 принимает сигнал в  $-70$  дБм, а уровень шума измеряется в  $-95$  дБм, то разница между принятым сигналом и фоновым шумом равна 25 дБ. Таким образом,  $SNR = 25$  дБ.

**РИСУНОК 13.2** Отношение Сигнал-Шум

Передача данных с очень низким SNR может быть повреждена. Если амплитуда уровня шума слишком близка к амплитуде принятого сигнала, то произойдет повреждение данных, и это вызовет повторные передачи [retransmissions] на 2ом Уровне. SNR в 25 дБ и выше считается хорошим качеством сигнала, а SNR в 10 дБ и ниже считается плохим или слабым качеством сигнала. SNR ниже 10дБ вероятно приведет к повреждению данных и скорости повторных передач до 50 процентов. Как показано на Рисунке 13.3, чтобы убедится, что кадры не повреждены из-за низкого SNR, большинство производителей БЛВС рекомендуют минимальный SNR в 20дБ. БЛВС уровня передачи голоса требует минимальный SNR в 25дБ, а более высокие уровни SNR нужны для более сложных способов модуляции квадратурной амплитудной модуляции [quadrature amplitude modulation (QAM)]. Принятый сигнал в -70 дБм будет на 20дБ или больше над уровнем шума в большинстве случаев. В большинстве сред сигнал в -70 дБм обеспечивает соединение с высокой скоростью передачи данных, а SNR 20 дБ гарантирует целостность данных. Высокий SNR также гарантирует, что радиомодули будут использовать модуляцию и схемы кодирования [modulation and coding schemes (MCSs)], которые дают более высокие скорости передачи данных. Более высокий SNR нужен, чтобы получить максимальные скорости передачи данных для клиентов 802.11ac, использующих модуляцию 256-QAM. Чтобы использовать преимущества модуляции и схем кодирования (MCSs), которые используют модуляцию 256-QAM, нужен SNR в 29 дБ или выше. Клиентские устройства 802.11ax требуют SNR в 35 дБ или выше, чтобы использовать модуляцию 1024-QAM.

**РИСУНОК 13.3** Рекомендации по SNR



VoWiFi связь является наиболее чувствительной к повторным передачам на 2ом уровне, чем трафик других типов приложений. Следовательно, при проектировании голосовых БЛВС, рекомендован сигнал -65 дБм или сильнее, так чтобы принятый сигнал был выше уровня шума. Даже если уровень шума будет очень высок -90 дБм, VoWiFi клиент с принятым сигналом -65 дБм будет все-еще иметь SNR 25 дБ. Всегда проверяйте рекомендации производителя клиента VoWiFi по принятому сигналу и SNR. Производитель может заявить, что достаточно принятого сигнала -67 дБм, а не -65 дБм. Дополнительно, разные производители VoWiFi могут советовать SNR в 28 дБ, вместо рекомендованного SNR в 25 дБ. При проектировании для голоса, SNR является наиболее важной радиометрикой [RF metric]. Также держите в уме, что в результате затухания на пути в свободном пространстве [free space path loss (FSPL)], фактическое расстояние

для клиентов –67 дБм будет меньше расстояния, чем для клиентов, получающих сигнал –70 дБм. Вспомните, что на каждые 3дБ потерь сила приемного сигнала уменьшается вдвое. Например, сигнал –70 дБм – это половина мощности сигнала –67 дБм. Клиенту нужно быть в непосредственной близости к ТД для принятого сигнала в –67 дБм.

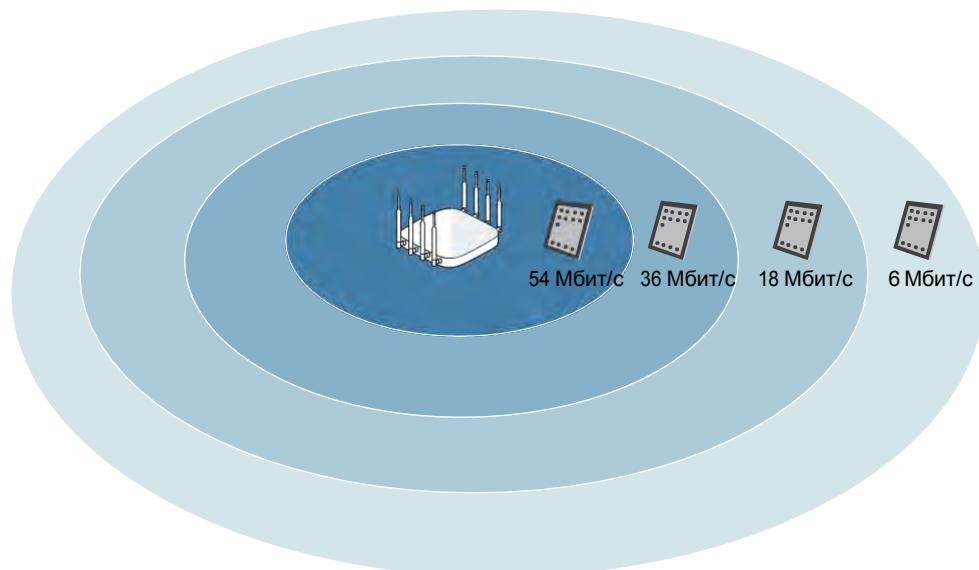
Так как полоса 2,4ГГц очень переполнена, уровень шума всегда выше, чему уровень шума в полосе 5ГГц. Следовательно, SNR чаще слишком низкий для голосовой связи или для использования сложной QAM модуляции. Полоса 2,4 ГГц обычно считается негарантированной [best-efforts] полосой для Wi-Fi уровня предприятия из-за зашумленной среды.

## Динамическое Переключение Скоростей

Будет ли клиентское устройство способно поддерживать связь с ТД, если сигнал упадет ниже –70 дБм? Ответ – да, потому что большинство клиентских устройств все еще могут декодировать преамбулу 802.11 из принятого сигнала, который всего лишь на 4 дБ над уровнем шума. По мере удаления радиомодулей мобильных клиентов от точки доступа, они будут переключаться вниз к низким возможностям пропускной способности, используя процесс, называемый *динамическое переключение скоростей* [*dynamic rate switching (DRS)*]. Скорость передачи данных между точкой доступа и клиентскими станциями будет переключаться вниз или вверх в зависимости от качества сигнала между двумя радиомодулями.

Существует прямая корреляция между качеством сигнала и расстоянием от ТД. По мере движения мобильных клиентских станций от точки доступа, и ТД и клиент будут переключаться вниз к меньшей скорости, которая требует менее сложную модуляцию и схему кодирования (MCS). В примере, изображенном на Рисунке 13.4, клиент 802.11a/g может подключиться на 54Мбит/с при приеме сигнала –70 дБм, но он может переключить передачу на низкую скорость передачи данных в 6Мбит/с, если сигнал намного слабее. Передача между двумя радиомодулями может быть 54Мбит/с на 9 метрах (30 футах), но 6Мбит/с на 27,4 метрах (90 футах).

**РИСУНОК 13.4** Динамическое переключение скоростей



Динамическое переключение скорости (DRS) также называется как *динамический сдвиг скорости [dynamic rate shifting]*, *динамический выбор скорости [dynamic rate selection]*, *адаптивный выбор скорости [adaptive rate selection]*, и *автоматический выбор скорости [automatic rate selection]*. Все эти термины ссылаются на метод сброса скорости на Wi-Fi приемнике (Rx) когда сила и качество входящего сигнала от передающего Wi-Fi радиомодуля уменьшается. Цель DRS переключение вверх или переключение вниз для оптимизации скорости и улучшения производительности. С клиентской точки зрения, более низкие скорости передачи данных обеспечивают большие концентрические зоны покрытия, по сравнению с зонами более высоких скоростей передачи данных.

Пороги, используемые для динамического переключения скорости являются проприетарными, и определяются производителями радиомодулей 802.11. Большинство возможностей DRS радиомодулей производителей привязано к порогам *индикатора силы принимаемого сигнала [receive signal strength indicator (RSSI)]*, частоте ошибок пакетов [*packet error rates*], и повторным передачам [*retransmissions*]. Метрики RSSI обычно основаны на силе сигнала и качестве сигнала. Другими словами, станция может переключиться вверх или вниз по скоростям передачи данных на основе силы принятого сигнала в дБм или значении сигнал-шум (SNR). Так как производители реализуют DRS по-разному, у вас могут быть два радиомодуля разных производителей в одном и том же месте; и пока один работает с точкой доступа на 300 Мбит/с, другой работает на 270Мбит/с. Например, один производитель может переключаться вниз со скорости передачи данных 156 Мбит/с до 52Мбит/с при -78 дБм, в то время как другой производитель может переключиться между теми же двумя скоростями при -81 дБм. Переключение скоростей также может быть основано на SNR. Еще раз, существует корреляция между качеством сигнала и расстоянием от ТД. Помните, что DRS работает со всеми Физическими Уровнями (PHYs) 802.11. То есть, устаревшие радиомодули 802.11b будут переключаться между четырьмя скоростями передачи данных 1, 2, 5.5, и 11 Мбит/с, в то же время радиомодуль 802.11n/ac/ax будет переключаться между более широким диапазоном доступных скоростей передачи данных.

Часто существует большое заблуждение, что только клиентские радиомодули используют динамическое переключение скоростей. Как уже упоминалось, клиентские радиомодули переключаются вниз на меньшие скорости передачи данных, если присутствует более слабый полученный сигнал от ТД. Однако, радиомодуль в точке доступа также использует динамическое переключение скоростей. Основываясь на силе входящего полученного сигнала от клиента, радиомодуль точки доступа переключает скорость передачи данных для передачи в нисходящем направлении к клиентскому радиомодулю. Слабый сигнал от входящего клиента приводит к переключению на более низкие скорости передачи данных для передачи в нисходящем канале [*downlink*] от ТД.

Мобильность может вызвать переключение в скоростях передачи данных. DRS обеспечивает способ радиомодулям ТД и клиентов продолжать работать с меньшими скоростями передачи данных, несмотря на слабый сигнал и низкий SNR. Однако, одна из основных целей проектирования покрытия БЛВС это обеспечить высокоскоростное соединение и ограничить насколько возможно переключение на низкие скорости передачи данных. Клиенты, которые переключаются вниз на низкие скорости передачи данных, потребляют больше эфирного времени [*airtime*] и влияют на общую производительность БЛВС. Вместо клиентского переключения на низкие скорости передачи данных, лучшим сценарием будет переключение клиента на другую ТД с сильным сигналом, и продолжить соединение с высокой скоростью передачи данных.

## Мощность Передачи

Заметный фактор, который влияет и на покрытие Wi-Fi и на роуминг - это мощность передачи точек доступа. Хотя большинство внутренних ТД могут иметь настройки максимальной мощности передачи в 100мВт, они редко устанавливаются на полную мощность. Высокая мощность передачи расширяет фактическую зону действия точки доступа; однако, проектирование БЛВС строго для зоны охвата является устаревшей концепцией. Позже в этой главе мы обсудим более высокие приоритеты проектирования емкости БЛВС и потребления эфирного времени. ТД с максимальной мощностью передачи приведут к избыточному покрытию и не будут соответствовать вашим потребностям по емкости. Точки доступа, установленные на полную мощность передачи внутри помещений, также увеличивают вероятность одноканальной интерференции, приводящей к появлению ненужной служебной информации [overhead] при борьбе за среду. Любая ТД с высокой мощностью передачи также увеличивает вероятность появления "залипших" клиентов [sticky clients], которые отрицательно влияют на роуминг, как обсуждается далее в Главе 15 "Поиск и устранение проблем БЛВС". Из-за всех этих причин типовые инсталляции Wi-Fi проектируются с ТД с установкой от одной четвертой до одной трети от максимальной мощности передачи. В некоторых случаях, среди с очень высокой плотностью пользователей могут требовать, чтобы мощность передачи ТД была установлена в наименьшую настройку в 1мВт.

Еще одним пунктом рассмотрения является мощность передачи клиентов. Одной жарко обсуждаемой темой является концепция сбалансированного по мощности канала связи между ТД и клиентом. Простыми словами, настройки мощности передачи между ТД и клиентом являются одинаковыми. Очень часто, Wi-Fi клиенты передают с более высокими уровнями мощности, по сравнению с внутренними точками доступа. Мощность передачи многих внутренних ТД может быть 10мВт или меньше из-за необходимости проектирования высокой плотности. Однако, большинство клиентов, таких как смартфоны и планшеты могут передавать с фиксированной амплитудой в 15мВт или 20мВт. Так как клиенты часто передают с большей мощностью, чем ТД, и так как клиенты мобильны, то одноканальная интерференция [co-channel interference (CCI)] часто вызывается несовпадением(несогласованностью) мощностей. Клиенты и ТД, которые поддерживают *контроль мощности передачи* [*transmit power control (TPC)*], обычно могут минимизировать эту проблему. Более детальное обсуждение ТРС можно найти в Главе 15.

## Проектирование Роуминга

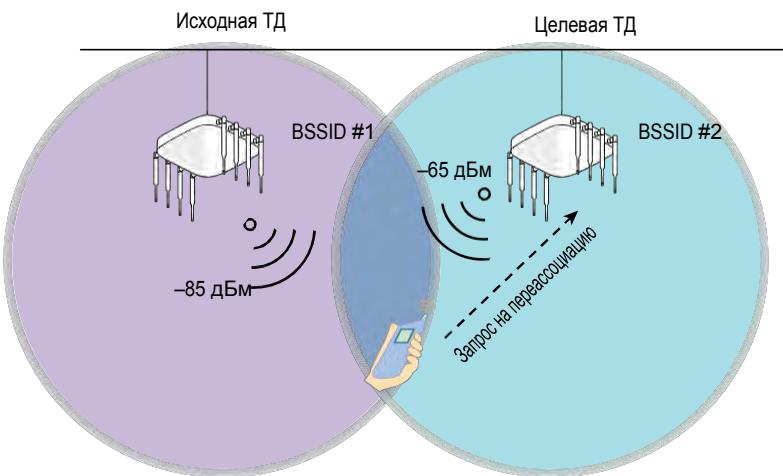
Как вы узнали из этой книги, *роуминг [roaming]* - это когда клиентская станция незаметно(бесшовно) перемещается между сотами радиопокрытия. Клиентские станции переключают связь по разным точкам доступа и переходят из исходного базового состава сервиса (BSS) в новый BSS. Бесшовная связь для клиентских станций, перемещающихся между зонами покрытия в расширенном составе сервиса (ESS), является жизненно необходимой для непрерываемой мобильности. Одна из наиболее обычных проблем, которую вам нужно решать - это проблема с роумингом. Проблемы роуминга обычно вызваны слабым дизайном сети.

Клиентские станции, не точки доступа, решают переключаться ли или нет клиенту между точками доступа. Некоторые производители могут привлекать точку доступа или контроллер БЛВС в процесс принятия решения о роуминге, но, в конечно счете, клиентская станция инициирует роуминговый процесс с кадра запроса на переассоциацию. Способ, которым клиентская станция принимает решение о роуминге, является набором собственных правил, определяемых производителем радиомодуля 802.11, обычно определяемых порогом запуска роуминга. Роуминговые пороги обычно включают силу сигнала, SNR, и частоту битовых ошибок. Когда клиентская станция поддерживает связь по сети, она продолжает искать другие точки доступа путем зондирования и прослушивания разных каналов, и слышит полученные сигналы от других ТД. Наиболее важным параметром всегда будет сила полученного сигнала; по мере того как принимаемый сигнал от исходной ТД становится слабее, а станция слышит более сильный сигнал от другой известной точки доступа, станция инициирует роуминговый процесс. Однако, другие метрики, такие как SNR, частота ошибок, повторные передачи могут также принимать участие в том, что заставляет клиента переключиться. SNR является метрикой, используемой некоторыми Wi-Fi клиентами, чтобы запустить события роуминга, а также динамического переключения скорости.

Как показано на Рисунке 13.5, по мере удаления клиентской станции от исходной точки доступа, с которой она ассоциирована, когда сигнал падает ниже предопределенного порога, то клиентская станция попытается подключиться к новой целевой точке доступа с более сильным сигналом. Клиент посыпает кадр, называемый *кадр запроса на переассоциацию [reassociation request frame]*, чтобы начать процедуру роуминга.

Глава 9, “802.11 MAC,” объясняет весь обмен кадров переассоциации более детально.

РИСУНОК 13.5 Роуминг

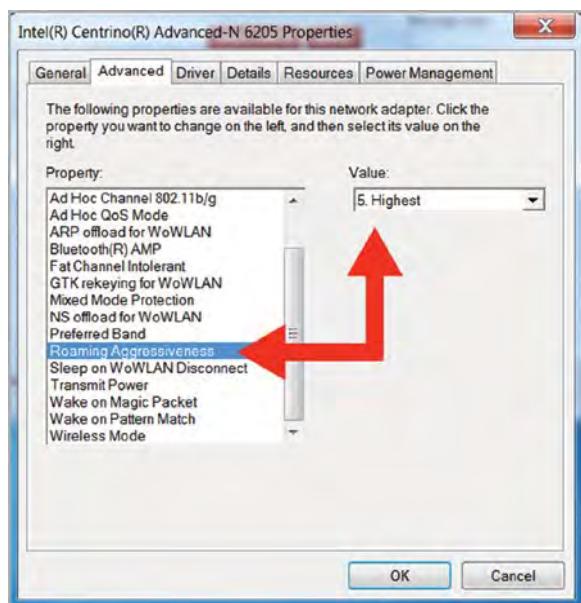


В зависимости от типа клиентского устройства БЛВС, пороги запуска роуминга могут быть очень простыми или совершенно сложными. Например, Wi-Fi смартфон может переключиться на новую ТД с сигналом на 5дБ сильнее, чем у ТД, с которой телефон ассоциирован. Телефон, переключившись на новую ТД, может требовать сигнал на 10дБ лучше, чтобы переключиться обратно на исходную ТД. Эти спусковые пороги [trigger thresholds] предназначены для предотвращения со стороны клиента пинг-понга с ассоциациями между двумя ТД. К сожалению, существует не так много опубликованных данных относительно триггерных роуминговых порогов. Однако, некоторые производители клиентов публикуют полезную информацию о роуминговых триггерах в руководствах по установке или на форумах поддержки. Вот несколько примеров:

- Устройства Apple macOS: <https://support.apple.com/en-us/HT206207>
- Устройства Apple iOS: <https://support.apple.com/en-us/ht203068>
- Мобильные устройства Samsung: <https://docs.samsungknox.com/admin/knox-platform-for-enterprise/kbas/kba-115013403768.htm>

Так как роуминг является проприетарным, клиентская станция определенного производителя может переключаться раньше, чем клиентская станция второго производителя по мере их движения через различные соты покрытия. Некоторые производители любят подталкивать к роумингу, в то же время другие запускают роуминг при более низких порогах принятого сигнала. В среде, где администратор БЛВС должен поддерживать радиомодули нескольких производителей, совершенно определенно будет наблюдаться различное поведение роуминга.

Знайте, что некоторые клиентские устройства предлагают возможность по настройке из роуминговых порогов триггеров вручную. Как показано на Рисунке 13.6, Wi-Fi радиомодуль Intel, находящийся во многих ноутбуках с Windows, имеет настраиваемые установки по агрессивности роуминга.



До поры до времени администратор БЛВС будет сталкиваться с уникальными вызовами из-за проприетарной природы роуминга. Однако, более новые клиенты могут использовать дополнительные параметры, такие как отчет о соседних ТД или загрузка емкости на ТД, чтобы помочь оптимизировать роуминговый процесс. Как обсуждалось в Главе 2 "Стандарты и Поправки IEEE 802.11", принятая поправка 802.11k определяет использование *измерение радио ресурса [radio resource measurement (RRM)]* и *отчеты о соседях [neighbor reports]*, чтобы улучшить производительность роуминга. Принятая поправка 802.11g также определяет быструю безопасную передачу клиента от ТД к ТД, когда происходит роуминг между сотами в беспроводной ЛВС, использующей сильную безопасность, определенную в надежной безопасной сети [*robust security network (RSN)*]. Поправка 802.11v определяет клиентские механизмы по изучению загрузки емкости ТД, которая может быть учтена при принятии решения о роуминге клиентом.

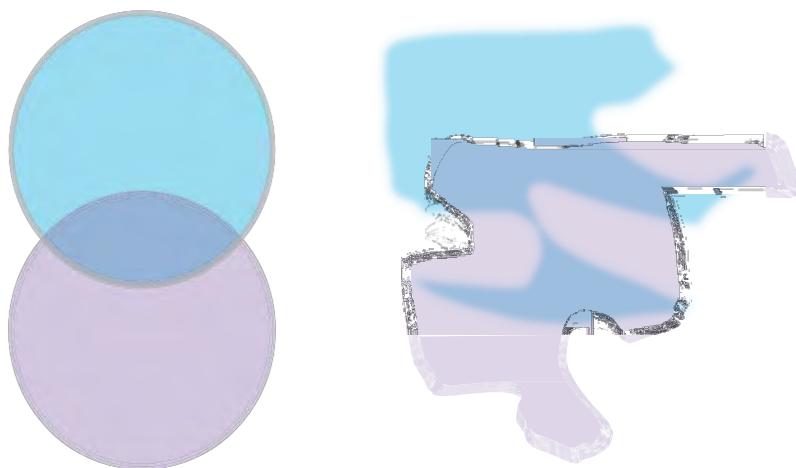
#### Поддержка механизмов 802.11k, 802.11r и 802.11v с клиентской стороны

Большинство производителей инфраструктуры БЛВС уже поддерживают технологии 802.11k/r/v в своих ТД и контроллерах, но многие клиентские устройства еще нет. Wi-Fi Альянс проверяет некоторые аспекты поправок 802.11k (управление ресурсом), 802.11r (быстрый безопасный роуминг), и 802.11v (беспроводное сетевое управление) в сертификации, называемой Голосовая связь уровня Предприятия [Voice-Enterprise]. Хотя сертификация Voice-Enterprise это реальность, большая часть устаревших 802.11a/b/g/n клиентов не поддерживают механизмы 802.11k/r/v. Однако, поддержка технологий 802.11k, 802.11r, и 802.11v с клиентской стороны выросло за последние годы для большинства мобильных устройств 802.11ac и 802.11ax.

## Первичное и Вторичное Покрытие

Лучший способ гарантировать, что бесшовный роуминг будет иметь место быть - это правильный дизайн и тщательное радиообследование места установки. Когда вы проектируете БЛВС 802.11, большинство производителей рекомендуют 15-30 процентное перекрытие областей покрытия в -70 дБм. Годами, руководства по проектированию БЛВС и листовки [white papers] от разных производителей БЛВС ссылались на 15-30 процентное пересечение зон покрытия, как показано слева на Рисунке 13.7. Проблема в том, как вычислить и измерить перекрытие зон? Следует ли использовать окружность, диаметр или радиус для измерения площади перекрытия зон? Дополнительно, листовки [white papers] производителей БЛВС (и даже эта книга) используют иллюстрации, чтобы изобразить зоны покрытия как идеально круглые. В действительности, зоны покрытия имеют странную форму, как амёба или вспышка в виде звезды. Как можно измерить перекрытие зон покрытия, если каждое покрытие имеет разную форму?

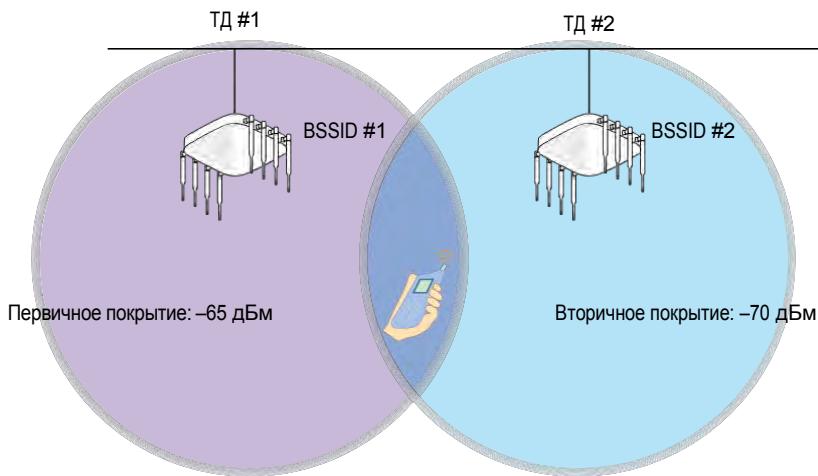
РИСУНОК 13.7 Перекрытие зон



Эксперт по радиообследованию Wi-Fi Кейт Парсонс [Keith Parsons], CWNE #3, годами проповедовал об ошибочности измерения перекрытия покрытия точек доступа. В действительности, перекрытие покрытия лучше всего определяется как дублированное или дублированное, первичное и вторичное, покрытие с точки зрения клиентской Wi-Fi станции. Должно быть проведено надлежащее контрольное радиообследование [validation survey], чтобы гарантировать, что клиент всегда будет иметь соответствующее дублированное покрытие от нескольких точек доступа. Другими словами, каждой клиентской Wi-Fi станции (STA) нужно слышать по крайней мере одну точку доступа с определенным RSSI и резервную или вторую точку доступа с другим RSSI. Обычно, большинство порогов RSSI от производителей требует принимаемый сигнал в -70 дБм для связи с более высокоскоростной передачей данных. Следовательно, клиентской станции нужно слышать вторую ТД с сигналом в -75 дБм или выше, когда сигнал, полученный от первой ТД, падает ниже -70 дБм. Единственный способ определить доступно ли надлежащее первичное/вторичное покрытие для клиентов - это проведение радиообследования объекта для анализа покрытия. Надлежащий дизайн покрытия и процедуры контрольного радиообследования детально обсуждаются в Главе 14.

Как показано на Рисунке 13.8, когда вы проектируете первичное и вторичное покрытие ТД, типовое правило следующее: ассоциированный с ТД потенциальный роуминговый клиент также слышит другую ТД в диапазоне 5дБ. Например, пока клиент подключен к ТД с расчетным покрытием –65 дБм, этот же самый клиент должен всегда слышать, по крайней мере, еще одну ТД с –70 дБм. Некоторые профессионалы по проектированию БЛВС предпочитают совпадающие силы сигналов, когда проектируют первичное и вторичное покрытие ТД. Например, пока клиент, ассоциированный с ТД с плановым покрытием –65 дБм, этот же самый клиент должен также всегда слышать, по крайней мере, еще одну ТД с –65 дБм. Это также гарантирует резервирование в случае поломки ТД.

**РИСУНОК 13.8** Первичное и вторичное покрытие



Роуминговые проблемы всегда будут происходить, если не достаточно дублированного покрытия зон. Слишком маленькое дублированное покрытие будет фактически создавать мертвую роуминговую зону, и связь может быть временно потеряна. С другой стороны, слишком много дублированных покрытий также приведет к роуминговым проблемам. Чего вы не хотите - это чтобы клиент мог слышать сильный сигнал –70 дБм от дюжины ТД из любой точки. Слишком много дублирующих покрытий может также создать ситуацию, в которой клиентское устройство постоянно переключается туда-сюда между двумя или более ТД на разных каналах.

Более того, слишком много ТД с сильными сигналами могут стать причиной проблемы залипшего клиента. Клиентская станция может оставаться ассоциированной с исходной ТД и не подключаться ко второй точке доступа, даже если мобильное устройство прямо под второй точкой доступа. Дополнительно, если клиентская станция слышит дюжину ТД на том же канале с мощными сигналами, произойдет деградация производительности из-за служебной информации при борьбе за среду.

## Быстрый Безопасный Роуминг

Другая проблема большой важности при проектировании роуминга это задержка. Стандарт 802.11-2020 предлагает использовать решение безопасности 802.1X/EAP на предприятиях. Среднее занимаемое время во время процесса аутентификации может быть 700 миллисекунд или больше.

Когда бы не переключалась клиентская станция на новую точку доступа, требуется повторная аутентификация [reauthentication], если развернуто решение по безопасности 802.1X/EAP. Задержка по времени, которая является результатом процесса аутентификации, может вызвать серьезные прерывания у чувствительных ко времени приложений. VoWiFi требует роуминговое переключение за 150 миллисекунд или намного меньше. Необходимо решение *быстрого безопасного роуминга* [*fast secure roaming (FSR)*], если безопасность 802.1X/EAP и чувствительные ко времени приложения используются вместе в беспроводной сети. IEEE определяет механизмы *быстрого перехода базового состава сервиса* [*fast basic service set transition (FT)*] в качестве стандарта для быстрого и безопасного роуминга. Процедуры FT(быстрого перехода) были впервые определены в поправке IEEE 802.11r-2008. Wi-Fi Альянс реализовал сертификацию Voice-Enterprise, которая определяет механизмы быстрого перехода [FT] и 802.11r. Хотя 802.11r уже примерно более 12 лет [а на момент перевода более 15 лет], ее принятие идет медленно. Однако, поддержка Voice-Enterprise с клиентской стороны стала более распространенной в последние годы.

Если планируется использовать безопасность 802.1X/EAP для клиентов с поддержкой голоса, то будет необходимо решение быстрого безопасного роуминга.

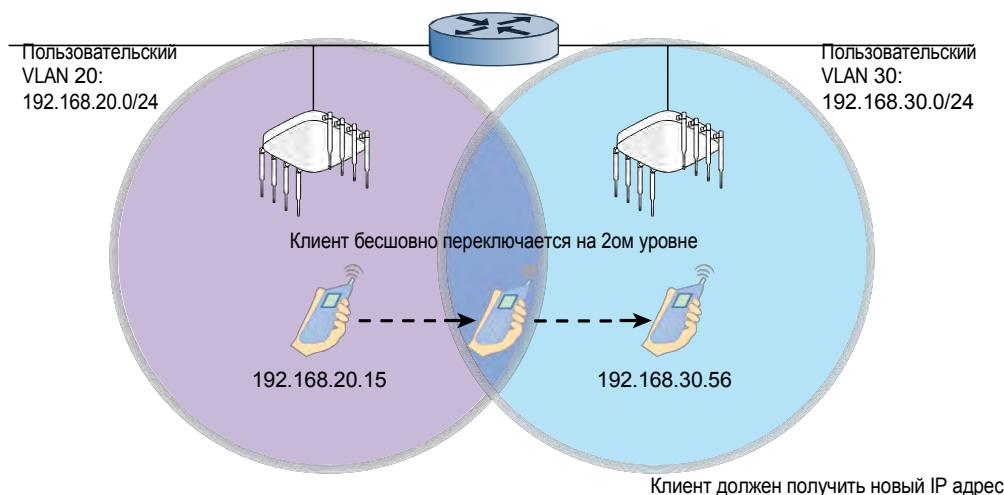


Ни нестандартные механизмы быстрого безопасного роуминга, например [opportunistic key caching (OKC)], ни стандартные роуминговые механизмы быстрого перехода BSS (FT) не проверяются на экзамене CWNA. Способы быстрого безопасного роуминга являются интенсивно проверяемой темой на экзамене Сертифицированный Профессионал Беспроводной Безопасности [Certified Wireless Security Professional (CWSP)].

## Роуминг 3 Уровня

Одно из главных размышлений при проектировании БЛВС - что произойдет, если клиентская станция при роуминге пересекает границы 3его уровня. Wi-Fi работает на 2ом уровне, и роуминг, фактически, процесс 2ого уровня. Как показано на Рисунке 13.9, клиентская станция переключается между двумя точками доступа

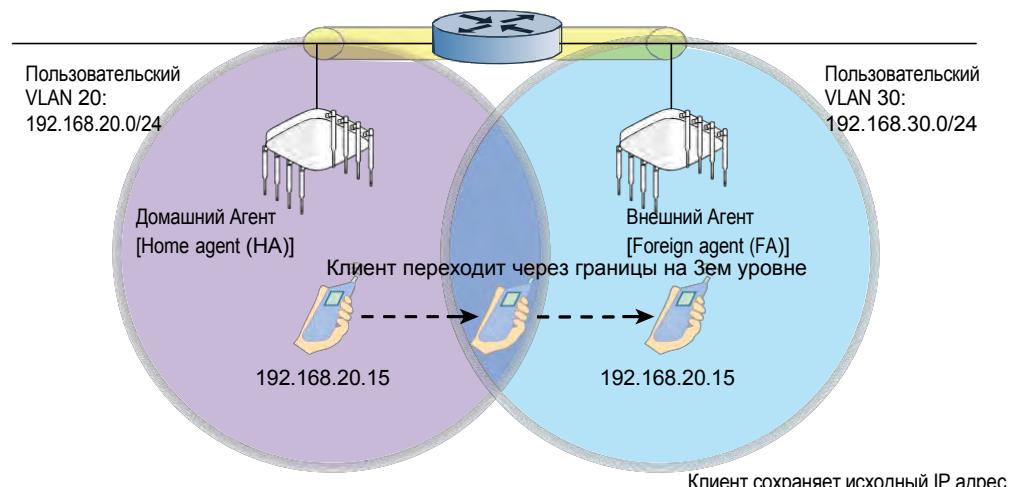
**РИСУНОК 13.9** Границы роуминга 3 уровня



Роуминг беспроводен на 2ом уровне, а пользовательские VLANы привязаны к разным подсетям на каждой стороне маршрутизатора. В результате, клиентская станция потеряет соединение на Зем уровне и должна будет получить новый IP адрес. Любые ориентированные на соединение приложения, которые работают, когда клиент переустанавливает соединение на Зем уровне, нужно будет перезапустить. Например, разговор по VoIP телефону разорвется в этом сценарии, и нужно будет снова перезванивать.

Так как беспроводные сети обычно интегрируются в уже существующие проводные топологии, то часто требуется пересечение границ Зего уровня, особенно при крупных установках. Единственный способ поддерживать связь на верхних уровнях при пересечении подсетей Зего уровня - это обеспечить решение по роумингу Зего уровня [*layer 3 roaming*], которое основано на стандарте *Мобильного IP* [*Mobile IP*]. Мобильный IP - это стандартный протокол Подразделения Инженерных Задач Интернета [Internet Engineering Task Force (IETF)], который позволяет пользователям мобильных устройств перемещаться из одной сети Зего уровня в другую с сохранением своей исходной IP адресации. Мобильный IP определен в IETF Request for Comments (RFC) 5944. Решения по роумингу на Зем уровне, основанные на Мобильном IP, используют некоторый тип туннелирования и инкапсуляции IP заголовка, чтобы позволить пакетам перемещаться между отдельными доменами Зего уровня, с целью поддержки связи на верхних уровнях. Большинство производителей БЛВС теперь поддерживают некоторый вид решения по роуминга на Зем уровне, как показано на Рисунке 13.10.

**РИСУНОК 13.10** Мобильный IP



Мобильный клиент получает IP адрес, называемый домашним адресом в домашней сети. Мобильный клиент должен зарегистрировать свой домашний адрес на устройстве, называемом *домашний агент* [*home agent (HA)*].

Как показано на Рисунке 13.10, точка доступа, с которой изначально ассоциирован клиент, выступает в качестве домашнего агента. Домашний агент - это единая точка контакта для клиента, когда он переключается (находится в роуминге) через границы на третьем уровне. Домашний агент [HA] делится информацией базы данных клиентских IP/MAC из таблицы, называемой *таблица домашнего агента* [*home agent table (HAT)*], с другим устройством, называемым *внешний агент* [*foreign agent (FA)*].

В этом примере внешний агент - это другая точка доступа, которая поддерживает все связи Мобильного IP с домашним агентом от имени клиента.

IP адрес внешнего агента называется *адресом пересылки* [*care-of address*]. Когда клиент осуществляет роуминг с пересечением границ Зого уровня, клиент переключается на внешнюю сеть, где расположен внешний агент (FA). FA использует таблицы домашнего агента (НАТ), чтобы найти местоположение домашнего агента (НА) клиентской мобильной станции. FA связывается с НА и устанавливает туннель Мобильного IP.

Любой трафик, который отправлен на домашний адрес клиента, перехватывается домашним агентом (НА) и отправляется через туннель Мобильного IP к внешнему агенту (FA). Затем FA доставляет туннелированный трафик клиенту, и клиент способен поддерживать соединение, используя исходный домашний адрес. В нашем примере, туннель Мобильного IP между двумя ТД с разных сторон маршрутизатора. Если пользовательские VLANы присутствуют на границе сети, туннелирование пользовательского трафика происходит между точками доступа, которые принимают на себя роли НА и FA. Туннелирование часто распределено между несколькими ТД. Однако, пользовательские VLANы могут находиться в DMZ или на уровне ядра сети с контроллером БЛВС. В среде с одним контроллером БЛВС роуминговое переключение с ТД на ТД на Зем уровне существуют как механизмы плоскости контроля в едином контроллере. В среде с несколькими БЛВС IP туннель создается между контроллерами, которые развернуты в разных маршрутизируемых границах в различных пользовательских VLANах. Один из контроллеров работает как домашний агент, а другой контроллер работает как внешний агент.

Хотя поддержка соединения на верхнем уровне возможна с этими решениями по роумингу на Зем уровне, увеличенная задержка иногда является проблемой. Кроме того, роуминг Зого уровня может и не требоваться вашей сети. Менее сложная инфраструктура часто использует простой дизайн 2ого уровня. В более крупных корпоративных сетях часто несколько пользовательских VLAN и VLANов управления связанных с несколькими подсетями; следовательно требуется решение по роумингу Зого уровня.

## Планирование Каналов

Еще один ключевой компонент проектирования БЛВС - это выбор надлежащих каналов для использования на нескольких ТД в одном и том же месте. Надлежащий канальный шаблон или дизайн переиспользования каналов нужны для гарантии бесшовного роуминга и для предотвращения двух типов интерференции, которые являются результатом ненадлежащего канального проектирования. Следующие разделы обсуждают основы проектирования каналов БЛВС.

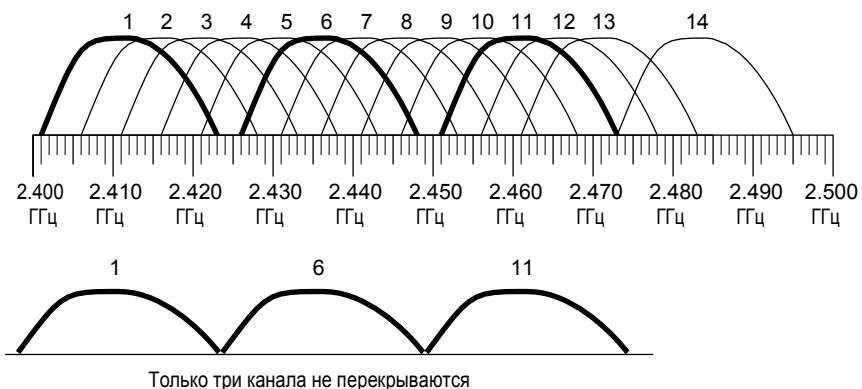
### Интерференция Смежных Каналов

Большинство производителей Wi-Fi используют термин *интерференция смежных каналов* [*adjacent channel interference (ACI)*] для описания деградации производительности в результате перекрывающегося частотного пространства, которое происходит из-за ненадлежащего планирования преиспользования каналов. В индустрии БЛВС, смежными каналами считаются следующий или предыдущий по номеру канал. Например, канал 3 является смежным с каналом 2.

Как вы узнали из Главы 6 "Беспроводные Сети и Технологии Расширения Спектра", стандарт 802.11-2020 требует расстояние в 25 МГц между центральными частотами каналов 2,4ГГц для того, чтобы они считались неперекрывающимися. Как изображено на Рисунке 13.11, если нужны три канала, то только каналы 1, 6 и 11 могут удовлетворять требованиям IEEE в ISM полосе 2,4ГГц в Соединенных Штатах

Некоторые страны позволяют использовать все 14 определенных IEEE 802.11 каналов в полосе ISM 2,4ГГц; однако, из-за положения центральных частот, не более трех каналов может быть использовано, избегая частотного перекрывания. Даже если все 14 каналов доступны, большинство профессионалов по проектированию БЛВС продолжают использовать каналы 1, 6 и 11 в полосе частот 2,4 ГГц.

**РИСУНОК 13.11** Неперекрывающиеся каналы 2,4ГГц



При проектировании беспроводного ЛВС вам нужны перекрывающиеся зоны покрытия для того, чтобы обеспечить роуминг. Однако, перекрывающиеся зоны не должны перекрываться по частотам, и в Соединенных Штатах только каналы 1, 6 и 11 должны быть использованы для наибольшей доступности неперекрывающихся каналов.

Перекрывающиеся зоны покрытия с перекрывающимися частотами приводят к, так называемой, интерференции смежных каналов. Если перекрывающиеся зоны покрытия имеют также пересечение по частоте от соседних каналов, то переданные кадры будут повреждены, приемники не будут отправлять АСК, и повторные передачи уровня 2 значительно увеличиваются.

## Переиспользование каналов 2,4 ГГц

Чтобы избежать интерференции смежных каналов, необходим план переиспользования каналов. Еще раз, перекрывающиеся по радио зоны покрытия нужны для роуминга, но нужно обязательно избегать перекрытия по частотам. Только три канала, которые удовлетворяют этим критериям в ISM полосе 2,4 ГГц - это каналы 1, 6 и 11 в Соединенных Штатах. ТД в полосе 2,4 ГГц, следовательно, должны всегда размещаться по шаблону *переиспользования каналов* [channel reuse pattern] аналогичному изображенному на Рисунке 13.12. Любой шаблон (или модель) переиспользования каналов БЛВС, которая использует три или более каналов, иногда называется как *многоканальная архитектура* [multiple- channel architecture (MCA)].

Вероятно самая большая ошибка, которую вы можете совершить при применении модели переиспользования каналов 2,4 ГГц, это дизайн, показанный на Рисунке 13.13. Обратите внимание, что все каналы являются смежными. Как ранее утверждалось, перекрывающиеся зоны покрытия, у которых также пересекаются частотные пространства от смежных зон, приведут к интерференции смежных каналов. Результат - поврежденные данные,

РИСУНОК 13.12 Модель переиспользования каналов в 2,4ГГц

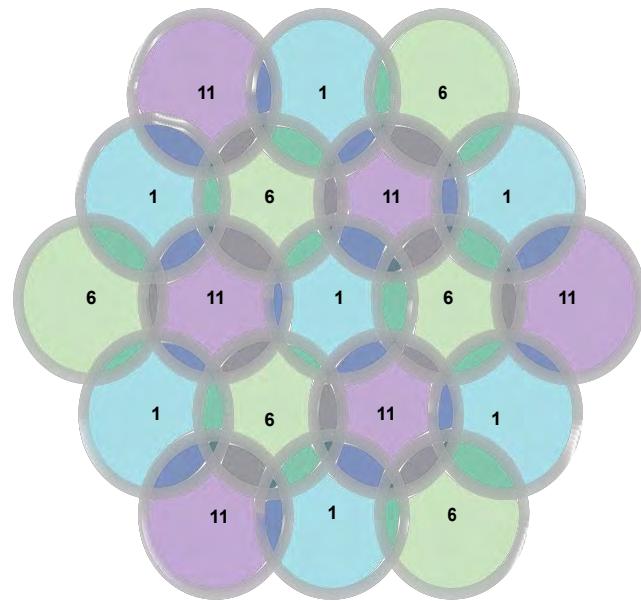
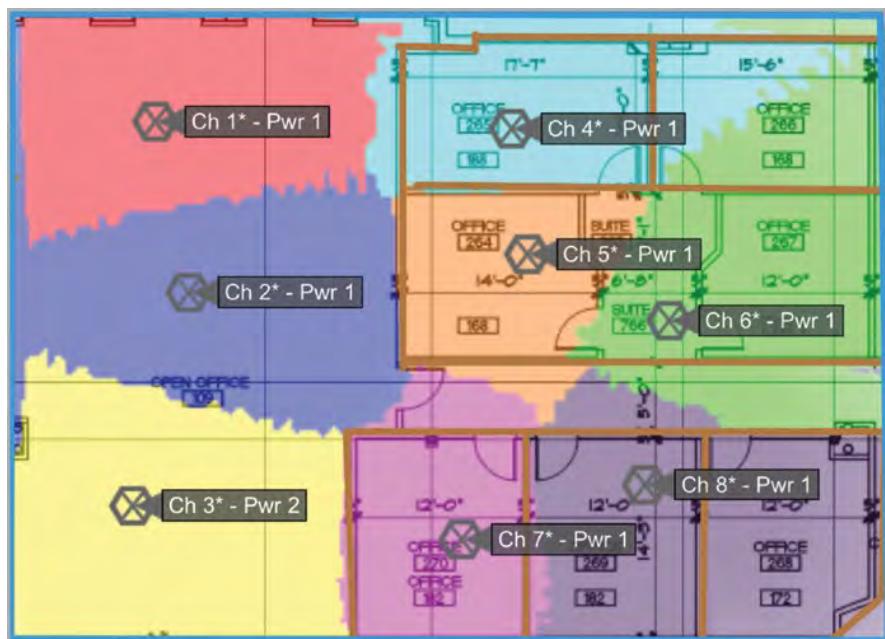


РИСУНОК 13.13 Ненадлежащий канальный дизайн - интерференция смежных каналов



повторные передачи 2 уровня, и экстремальная деградация производительности. В этом сценарии, интерференция смежных каналов - это просто радио интерференция, вызванная вашей собственной ТД, из-за ненадлежащего канального планирования. Нужно любой ценой избегать ненадлежащий канальный план, изображенный на Рисунке 13.13.

Необходимо всегда думать трехмерно при проектировании многоканальной архитектуры модели переиспользования. Если точки доступа развернуты на нескольких этажах в одном здании, нужна будет модель переиспользования, как показано на Рисунке 13.14.

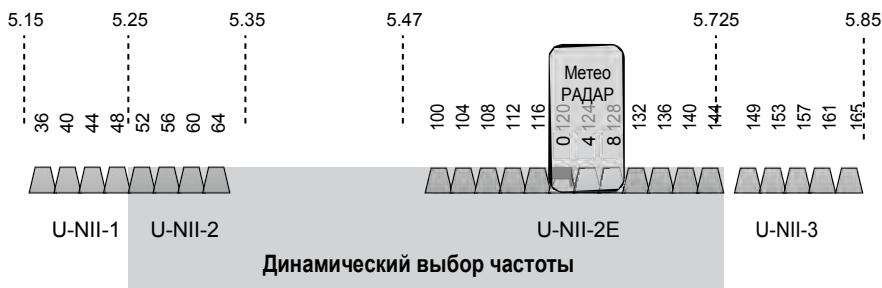
Распространенная ошибка - это развертывание шаблонного проекта путем выполнения радиообследования только на одном этаже и затем устанавливая точки доступа на тех же каналах и в тех же местах на каждом этаже. Точки доступа нужно размещать в шахматном порядке для трехмерной модели переиспользования. Также, зона покрытия в  $-70$  дБм каждой точки доступа не должна выходить далее одного этажа выше и ниже от этажа, где размещена точка доступа. Неправильно всегда предполагать, что покрытие проникающее на другие этажи обеспечит достаточную силу и качество сигнала. В некоторых случаях, перекрытия бетонные или стальные и пропускают очень мало , если вообще пропускают, сигнал покрытия. В результате, контрольное подтверждающее радиообследование является абсолютным требованием. Всегда помните, что радиоволны распространяются во всех направлениях. У некоторых коммерческих предиктивных инструментов радиоволнового моделирования, например iWave Design, есть возможность изобразить радиопокрытие в трехмерном виде.

**РИСУНОК 13.14** Трехмерное переиспользование каналов



Намного больше каналов доступно в полосах 5 ГГц U-NII, как показано на Рисунке 13.15. Все эти каналы технически считаются не перекрывающимися, так как присутствует разнос в 20МГц между центральными частотами. В действительности, будет присутствовать некоторое перекрытие по частотам на боковых полосах соседних OFDM каналов. Хорошая новость в том, что вы не ограничены только тремя каналами; намного больше каналов может быть использовано в модели переиспользования каналов в 5 ГГц, которая обсуждается далее в этой главе.

**РИСУНОК 13.15** Каналы в 5 ГГц



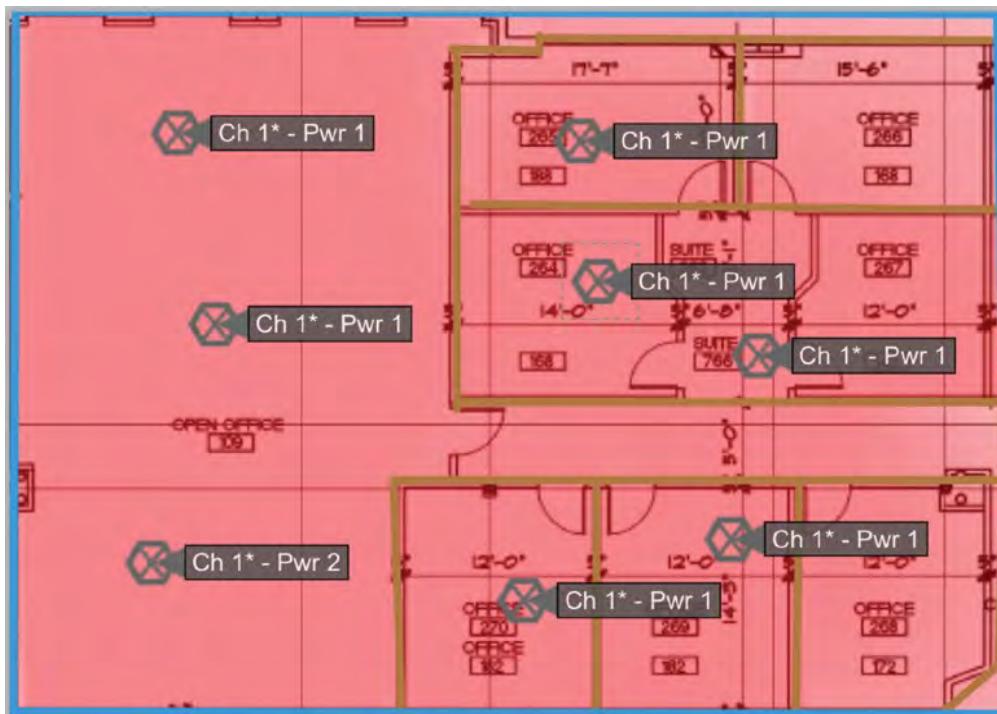
## Одноканальная Интерференция

Еще одна из наиболее распространенных ошибок, которую делают предприятия при первом развертывании БЛВС - это настройка точек доступа на один и тот же канал. Если все ТД на одном канале, то появляется переизбыток ненужной служебной информации при борьбе за среду. Как вы уже знаете, CSMA/CA декларирует полудуплексную связь, и только один радиомодуль может передавать на одном и том же канале одновременно.

Рисунок 13.16 изображает несколько близких ТД настроенных на передачу на канале 1. Если, ТД на канале 1 ведет передачу, все рядом стоящие точки доступа и клиенты на том же канале в радиусе слышимости отложат свои передачи. Результат - неблагоприятное влияние на пропускную способность. Близкие ТД и клиенты будут ждать намного дольше, чтобы передать, так как они должны получить свою очередь. Ненужная служебная информация (оверхед) при борьбе за среду, которая появляется из-за того, что все ТД на одном и том же канале, называется *со-канальная* или *одноканальная интерференция [co-channel interference (CCI)]*. В действительности, радиомодули 802.11 работают точно, как определено механизмами CSMA/CA, и это поведение, по идее, должно называться со-канальной или одноканальная совместная работа (кооперация). Ненужная служебная информация при борьбе за среду вызванная одноканальной интерференцией является результатом того, что ТД или клиенты слышат друг друга и откладывают передачи.

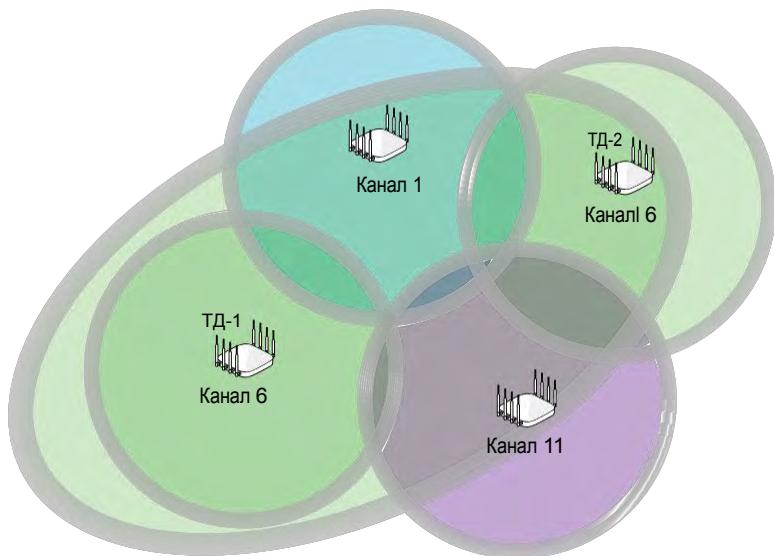
Одноканальная интерференция (CCI) является первой причиной ненужного потребления эфирного времени [*airtime*], которое может быть минимизировано лучшими практиками надлежащего проектирования БЛВС. Хорошая новость в том, что большинство проектировщиков БЛВС понимают, что не нужно настраивать все ТД на один и тот же канал. Более того, возможности адаптивного радио [*adaptive RF*], находящиеся в ТД производителей БЛВС уровня предприятия также автоматически выбирают каналы 1, 6 и 11 для радиомодулей 2,4ГГц. Первичная цель моделей переиспользования каналов в предотвращении одноканальной интерференции. План переиспользования каналов уменьшает потребление эфирного времени путем изолирования частотных доменов (каналов).

**РИСУНОК 13.16** Ненадлежащее переиспользование канала - одноканальная интерференция

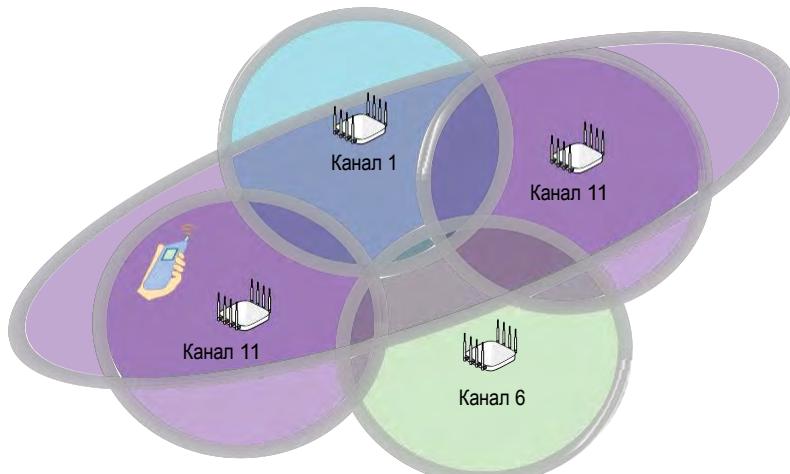


Плохая новость, однако, в том что одноканальную интерференцию почти невозможно предотвратить в полосе 2,4ГГц, потому что доступно только три канала для модели переиспользования. Остановиться ли радиосигнал на краю зоны покрытия, спроектированной для покрытия в -70 дБм? Ответ - нет, радиосигнал продолжит распространяться, и сигнал может быть услышан другими радиомодулями 802.11 на далеком расстоянии. Радиомодуль 802.11 отложит передачу, если он слышит передачу преамбулы физического (PHY) уровня другого радиомодуля 802.11 с порогом обнаружения сигнала [signal detect (SD)] всего лишь в 4 децибела (дБ) или выше над уровнем шума. Любой радиомодуль, который слышит другой радиомодуль на том же канале задержит передачу, что приведет к избыточной служебной информации при борьбе за среду и задержке.

Как показано на Рисунке 13.17, несмотря на трехканальную модель переиспользования, Точки Доступа на одном и том же канале будут слышать друг друга и откладывать передачу. Например, если ТД-2 на канале 6 слышит передачу преамбулы близкой ТД-1, также передающей на канале 6, ТД-2 притормаживает и не передает в это же самое время. Таким же образом, все клиенты, ассоциированные с обоими ТД, должны отложить передачу, если они слышат преамбулу передачи ТД-1. Все эти отерочки создают избыточную служебную информацию (оверхед) борьбы за среду и потребляют ценнное эфирное время, потому что у вас два базовых состава сервиса на одном и том же канале могут слышать друг друга. Одноканальная интерференция также часто называется как перекрывающийся базовый состав сервиса [*overlapping basic service set (OBSS)*].

**РИСУНОК 13.17** Одноканальная интерференция—Точки Доступа

В действительности, клиенты Wi-Fi являются первичной причиной OBSS и CCI интерференции. Как показано на Рисунке 13.18, если клиент, ассоциированный с ТД-1, передает на канале 11, то возможно, что ТД-2 (и любой клиент, ассоциированный с ТД-2) услышит преамбулу PHY клиента и должна будет отсрочить любую передачу. Что большинство людей не понимают о CCI - это тот факт, что клиенты являются причиной номер один CCI. Вам следует понимать, что CCI не статична, а всегда изменяется из-за мобильности клиентских устройств.

**РИСУНОК 13.18** Одноканальная интерференция—клиенты

Из-за того факта, что только три канала доступны в полосе 2,4ГГц, и потому что ССI вызывается клиентами, ССI практически неизбежна в полосе 2,4ГГц.

Одна стратегия, чтобы уменьшить ССI в полосе 2,4 ГГц - это выключить большинство радиомодулей 2,4ГГц в двухдиапазонных точках доступа и больше полагаться на покрытие, обеспечиваемое радиомодулями ТД 5 ГГц, для удовлетворения необходимости клиентской плотности. Хотя почти невозможно предотвратить ССI в полосе 2,4 ГГц, потребление эфирного времени, которое является результатом ССI, может быть минимизировано и возможно устранено с хорошим проектированием БЛВС в 5 ГГц, которое будет обсуждаться позже в этой главе.

Пожалуйста, не перепутайте интерференцию смежных каналов и одноканальную интерференцию. Интерференция смежных каналов - это просто результат ненадлежащего планирования каналов в полосе 2,4 ГГц, и может быть устранена путем использования только каналов 1,6 и 11. Интерференция смежных каналов является более серьезной проблемой, чем одноканальная интерференция, из-за повреждения данных и повторов на 2ом уровне.

В Европе и других регионах мира, больше каналов легально доступны для безлицензионной связи в полосе ISM 2,4 ГГц. В Европе, иногда применяется четырехканальная модель переиспользования каналов 1, 5 , 9 и 13. Хотя существует небольшое количество частотного перекрытия между этими четырьмя каналами, производительность в некоторых случаях может быть лучше, если служебная информация при борьбе за среду одноканальной интерференции может быть уменьшена из-за меньших утечек покрытия. Четырехканальный план все же имеет недостатки:

- Если соседнее предприятие развернет ТД по традиционному плану 1-6-11, то соседские ТД станут причиной серьезной интерференции смежных каналов с вашими ТД, развернутыми по плану 1-5-9-13.
- Также, все радиомодули Северной Америки ограниченный программным обеспечением и не могут передавать на канале 13. Любой приехавший к вам заказчик или сотрудник с ноутбуком, iPad или другим мобильным устройством, которое было приобретено в Северной Америке, не сможет подключиться к Европейской точке доступа, передающей на канале 13.

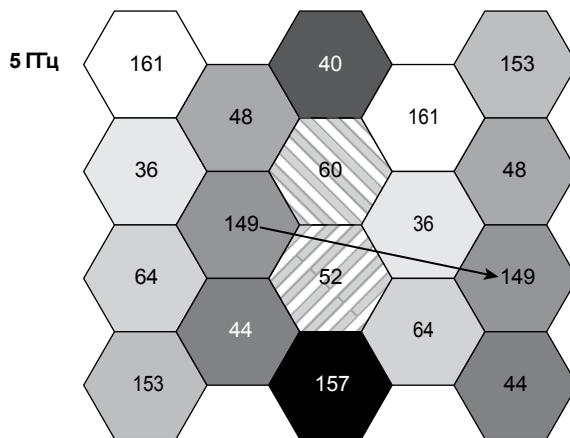
По этим причинам, обычно разворачивается более традиционный трехканальный план для 2,4 ГГц в Европе и других регионах мира

## Переиспользование Каналов 5 ГГц

До сих пор мы в основном фокусировались на проектировании переиспользования каналов для полосы 2,4 ГГц. Модели переиспользования каналов также следует использовать и в полосах частот 5ГГц. Если все каналы 5 ГГц официально доступны для передачи, то всего может быть доступно 25 каналов для модели переиспользования каналов.

В зависимости от региона, и других доводов, 9 каналов, 13 каналов, 22 канала, 25 каналов или другие комбинации могут быть использованы для моделей переиспользования каналов для 5 ГГц. Например, Рисунок 13.19 изображает 5 ГГц модель переиспользования каналов, используя большинство из не-DFS каналов, доступных в полосах U-NII-1 и U-NII-3. Однако, ключ для лучшего 5 ГГц дизайна переиспользования - это использовать насколько возможно больше каналов, включая каналы DFS.

**РИСУНОК 13.19** Модель переиспользования 5ГГц каналов (не-DFS каналы)



Расстояние до ячейки с тем же номером канала, по крайней мере, две ячейки.

При планировании модели переиспользования 5ГГц каналов следует принимать во внимание несколько факторов и лучших практик:

- Первый фактор для рассмотрения – это какие каналы официально доступны в вашей стране или регионе. В Европе, модель переиспользования большинства каналов в полосах U-NII-1, U-NII-2, и U-NII-2E является достаточно распространенной. В прошлом, у многих стран в Европе не было каналов в полосе U-NII-3 для безлицензионной связи. Некоторые Европейские страны разрешили передачу в полосе U-NII-3 при покупке недорогой лицензии. Последние годы, многие страны в Европе открыли полосу U-NII-3 для Wi-Fi и другой безлицензионной радиосвязи. Однако, каналы U-NII-3 часто продолжают не использоваться в установках на Европейских предприятиях, потому что устаревшее, но работающее, клиентское оборудование не поддерживает каналы. В итоге, план переиспользования каналов должен использовать все 5 ГГц каналы, доступные в регионе.
- Второй фактор для рассмотрения - это какие каналы в 5ГГц поддерживаются вашими клиентскими устройствами. Более старые клиенты очень часто не поддерживают каналы 144 или 165. Некоторые очень старые клиенты не поддерживают 5ГГц DFS каналы. Иногда вы можете обнаружить, что некоторые потребительского класса клиенты не передают на каналах DFS. Как ранее утверждалось, более старые клиенты в Европе могут не поддерживать каналы в полосе U-NII-3. Хорошая новость в том, что сегодняшние клиенты должны поддерживать все каналы 5ГГц, которые официально разрешены в вашем конкретном регионе.
- Хотя по определению IEEE, все 5ГГц каналы считаются неперекрывающимися, в действительности существует некоторое перекрытие частот боковых полос от смежных каналов. Рекомендуемая практика, чтобы любые смежные зоны покрытия использовали частоты, которые, по крайней мере, находятся на два канала друг от друга и не используют соседние частоты. Другими словами, не организовывать покрытие на ТД, передающей на канале 36, рядом с ТД, передающей на канале 40.

Однако, ТД, передающая на канале 36, смежная с ТД, передающей на канале 48, приемлема. Следование этому простому правилу предотвратит интерференцию смежных каналов от перекрытия боковой полосы.

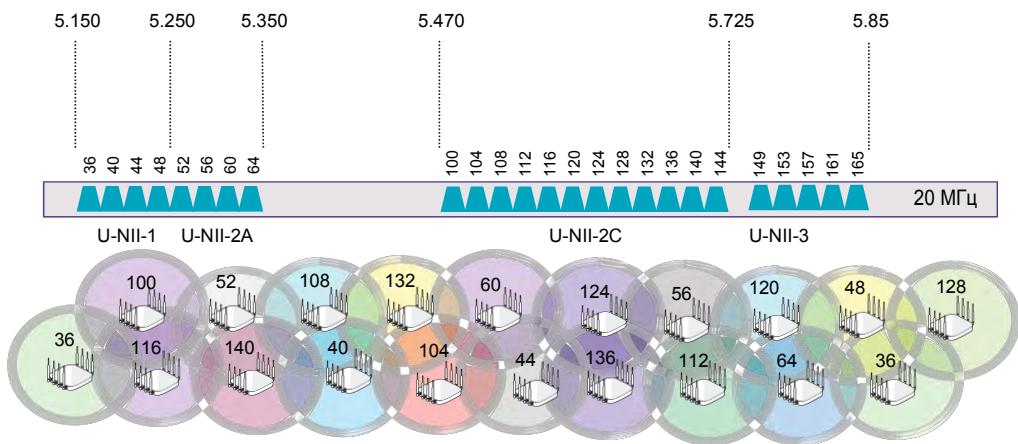
- Рисунок 13.19 также показывает, что вторая рекомендованная практика для проекта переиспользования каналов 5 ГГц в том, что должно быть, по крайней мере, расстояние в две зоны покрытия между любыми двумя точками доступа, передающими на одном и том же канале. Следование этому правилу должно минимизировать одноканальную интерференцию между ТД. Однако, это не обязательно может предотвратить одноканальную интерференцию от клиентов — и запомните, что клиентские передачи являются основной причиной ССI (одноканальной интерференции).
- Всегда, когда это возможно, используйте столько каналов в 5 ГГц сколько возможно, чтобы уменьшить ССI. Чем больше используемых каналов, тем больше вероятность, что ССI можно предотвратить, включая одноканальную интерференцию, которая происходит от клиентских устройств. Рисунок 13.20 изображает модель переиспользования каналов, часто используемую в Европе. Обратите внимание на пространственное расстояние между зонами покрытия обеих ТД, использующих канал 36. Когда вы также учтете фактор затухания в стенах, то вероятность того, что клиенты, ассоциированные с другой ТД на канале 36, услышат друг друга и отложат передачу будет скорее всего исключена. Модель переиспользования каналов для Соединенных Штатов может также включать пять дополнительных каналов, доступных в полосе U-NII-3.
- В большинстве случаев, вы можете использовать каналы с динамическим выбором частоты [dynamic frequency selection (DFS)]. Хорошая новость - это то, что большинство сегодняшних клиентских устройств могут передавать на каналах DFS, и включение каналов DFS в модель переиспользования каналов становится более распространенной. Единственная причина, чтобы не использовать каналы DFS - это, если огромная часть ваших клиентов состоит из устаревших устройств, которые не поддерживают каналы DFS.
- Если передачи от рядом находящегося радара вызывают переключение ваших ТД и клиентов на не-DFS каналы, просто исключите проблемные DFS каналы из проекта переиспользования каналов в 5 ГГц.

## Каналы DFS

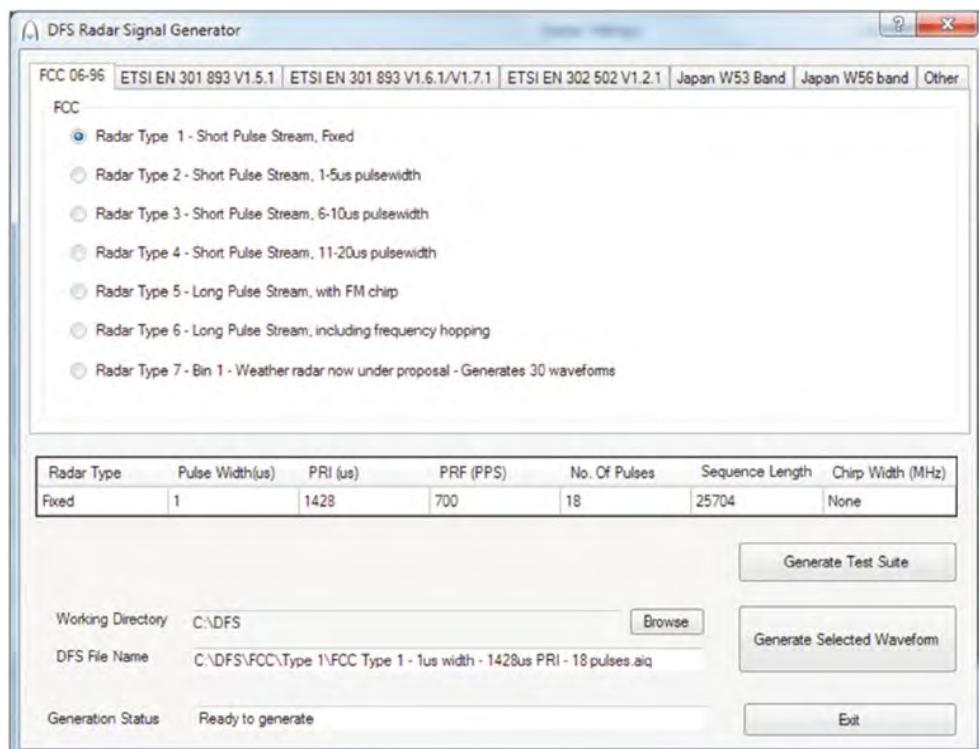
Как показано ранее на Рисунке 13.14, все каналы в полосе U-NII-2 (5.25–5.35 ГГц) и полосе U-NII-2e (5.47–5.725 ГГц) называются каналами *динамического выбора частоты* [dynamic frequency selection (DFS)]. Как вы раньше узнали, радиомодули БЛВС, работающие в этих 5 ГГц полосах, должны поддерживать DFS, чтобы предотвратить интерференцию от связи БЛВС с военными или метеорологическими радарными системами. Если импульсы радара обнаружены в любом из этих DFS каналов, то точкам доступа и клиентам не разрешено передавать на том же канале. Правила для радиомодулей 802.11 по передаче на DFS каналах может варьироваться от региона; однако, цель - избежать интерференции с радаром. Многие радарные системы защищены официальными правилами DFS, включая радары на судах, метео радары, и военные радары. Обратите внимание, что требования DFS применяются не только к радиомодулям Wi-Fi.

Регулирующие радиочастоты организации, такие как FCC в Соединенных Штатах и ETSI в Европе, отвечают за определение требований DFS, а также тестирование радиомодулей Wi-Fi на соответствие. Как показано на Рисунке 13.21, сурвое

**РИСУНОК 13.20** Предотвращение CCI в модели переиспользования каналов в 5 ГГц



**РИСУНОК 13.21** Волновые формы импульсов радара

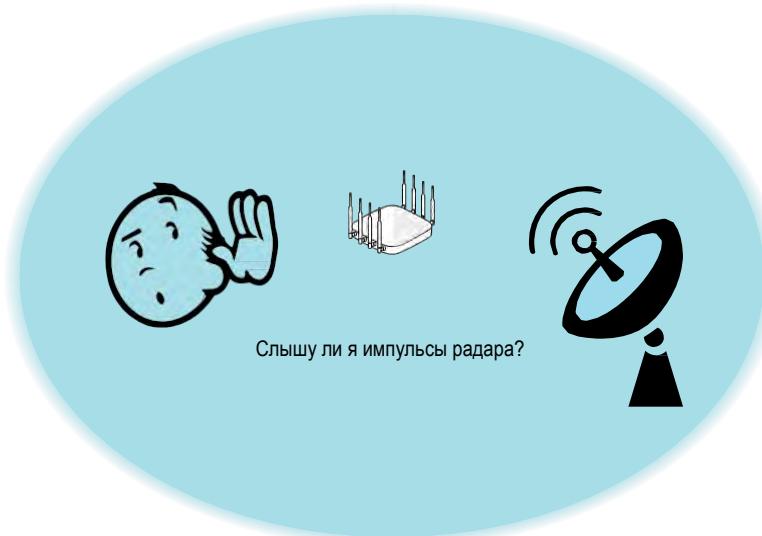


сертификационное испытание проводится для подтверждения, что радиомодули могут обнаруживать импульсы радара, а также соблюдать правила предотвращения интерференции. Радиомодули проверяются на различные уровни требуемой чувствительности по обнаружению импульсов радара. Для сертификации DFS проверяется шесть типов различных радарных волновых форм (пять коротких импульсов и один длинный импульс). Требуются минимальные проценты успешных обнаружений по определенным повторяющимся испытаниям. Держите в голове, что правила и тестирование DFS варьируются от региона.

Обычно регулирующие организации проверяют ТД на обнаружение импульсов радаров. Регулирующие радиочастоты организации определяют и головное устройство [master device] и клиентские устройства при проведении испытаний по сертификации DFS. Головное устройство [master device] это любое радиооборудование (как ТД), которое имеет функцию контроля обнаружения радара в скоординированной системе. Для головных устройств [master devices] требуется DFS сертификация. Клиентское устройство [client device]- это любое устройство, которое требует разрешения (авторизации) от головного устройства, чтобы начать связь на канале. Никакого обнаружения радара не нужно, если клиентское устройство контролируется головным устройством (ТД). Головное устройство должно поддерживать функциональность *проверки доступности канала [channel availability check (CAC)]*. CAC - это обязательный период времени, в течении которого ТД мониторит (отслеживает) канал, чтобы определить, превышает ли сигнал[waveform] радара определенный порог обнаружения DFS.

Вы могли заметить, что по-умолчанию, каналы DFS не включены в Wi-Fi ТД от производителя. Есть две причины, по которым каналы DFS обычно отключены по-умолчанию. Первая, окончательное решение использовать ли или нет каналы DFS в модели переиспользования в 5 ГГц зависит от заказчика или системного интегратора, который проектирует и развертывает ТД. Вторая, радиомодули новых ТД и клиентов должны быть сертифицированы FCC и другими регулирующими органами. В Европе и других регионах процесс сертификации быстрый, и DFS каналы доступны для передачи, когда новые ТД уровня предприятия выходят на рынок. Однако, в Соединенных Штатах, сертификация ТД для передачи на каналах DFS отделена от сертификации на не-DFS каналах. В результате, присутствует шестимесячная задержка с DFS сертификацией в Соединенных Штатах, что означает, что когда производитель Wi-Fi выпускает новые модели ТД, они не могут поддерживать каналы DFS в следующие шесть месяцев. После сертификации, обновление программного обеспечения ТД сделает каналы DFS доступными для использования. Следовательно, вы часто не видите, чтобы каналы DFS использовались на предприятии. На новых ТД изначально установленных на использование только не-DFS 5ГГц каналов, в дальнейшем каналы DFS никогда не используются. Однако, как вы узнали ранее в этой главе, включение DFS каналов в 5 ГГц модель переиспользования каналов является выгодным, потому что помогает минимизировать CCI путем предоставления большего количества каналов для проектирования модели переиспользования.

Итак, как точно работает DFS? Как изображено на Рисунке 13.22, перед тем как, ТД начнет передачу первый раз на DFS канале, она должна выполнить начальную проверку доступности канала [channel availability check (CAC)]. Радиомодуль ТД должен слушать в течении периода времени САС в 60 секунд, прежде чем будет разрешено передавать на канале. Если обнаружен какой-либо импульс радара, ТД не может использовать этот канал, и должна попробовать другой канал. Если никакого радара не обнаружено в течении первоначального 60и секундного САС периода прослушивания, то ТД может начать передачу кадра управления типа маяк [beacon management frames] на канале. В Европе, правила еще более строгие для каналов 120, 124, и 128 Терминалного Доплеровского Метеорологического Радара [*Terminal Doppler Weather Radar (TDWR)*]. ТД должна слушать целых 10 минут прежде, чем сможет передавать в частотном пространстве TDWR.

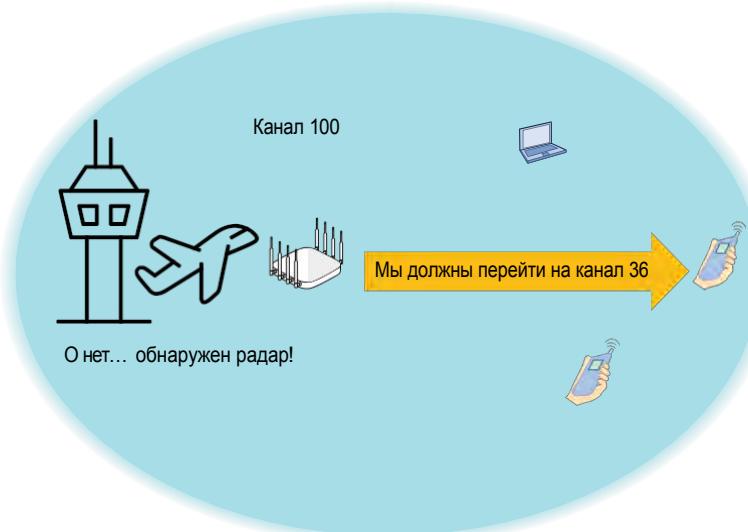
**РИСУНОК 13.22** Проверка доступности канала (CAC)

Клиентские радиомодули 802.11 должны также подчиняться правилам избегания радаров; следовательно, они обычно не будут изначально отправлять зондирующие запросы [probe request] ни по одному каналу DFS. Когда клиентские радиомодули сканируют каналы DFS и слышат, что ТД передает маяк [beacon] на этом канале DFS, клиент предполагает, что канал чист от радара и может начать аутентификационный и ассоциационный обмен кадрами с ТД.

Пожалуйста, поймите, что мониторинг радара непрерывен. Если ТД и клиенты уже работают на канале DFS, и обнаружен импульс радара, то ТД и все ассоциированные клиенты должны покинуть канал. Как показано на Рисунке 13.23, если обнаружен радар на текущей DFS частоте, то ТД информирует все ассоциированные клиентские станции о переходе на другой канал, используя кадр оповещения о смене канала [*channel switch announcement (CSA)*]. Информация об информационном элементе CSA может быть найдена в трех типах кадров управления: кадрах действия [action frames], кадрах-маяках [beacon frames], и кадрах ответов на зондирующие запросы [probe response frames]. У ТД и клиентов есть 10 секунд, чтобы покинуть DFS канал. ТД может послать несколько кадров CSA, чтобы гарантировать, что все клиенты ушли. Кадр CSA информирует клиентов, что ТД переходит на новый канал, и что они должны уйти на этот канал тоже. В большинстве случаев, на канал, который является не-DFS каналом. Некоторые производители предлагают возможность администратору БЛВС указать *запасной* канал для DFS [*DFS fallback*].

ДоНе перепутайте изменение канала ТД в результате обнаружения радара с изменением канала ТД, которое может быть запущено протоколом адаптивного управления радио ресурсом [adaptive radio resource management (RRM)] производителя Wi-Fi. Обнаружение радара требует, чтобы ТД и клиенты перешли на другой канал. Однако, протоколы RRM обычно учитывают DFS, потому что радарные события и DFS-обязывающие изменения канала могут повлиять и на сиюминутное и на будущее решения RRM. Протоколы RRM обсуждаются более детально позже в этой главе. И хотя DFS функциональность является обязательной, вы должны понимать, что производители БЛВС часто реализуют механизмы

**РИСУНОК 13.23** Оповещение о переключении канала (CSA)



DFS по-разному. На Рисунке 13.24 показан хороший диагностический инструмент по тестированию возможностей DFS ТД любого производителя – «WiFiMETRIX DFS diagnostic tool» доступный на [www.nutsaboutnets.com](http://www.nutsaboutnets.com).

Раз уж ТД и клиенты переключились на не-DFS канал, они не могут вернуться на предыдущий DFS канал, по крайней мере, еще 30 минут. Это называется *время не-занимания [non-occupancy time]*. Еще одна проблема возвращения на исходный DFS канал в том, что после 30-минутного периода ожидания ТД снова будет мониторить DFS канал в течении 60 секунд прежде, чем снова вести передачу. Это значит, что будет по крайней мере 60 секундный интервал, когда ТД не будет обслуживать клиентов. Один из производителей чипсетов, Broadcom, предлагает решение, называемое *DFS с нулевым ожиданием [zero-wait DFS]*, чтобы решить эту проблему, используя радиоцепи MIMO 5 ГГц радиомодуля точки доступа. Например, ТД 4×4:4 может слушать на DFS канале 104 одной радиоцепью MIMO, продолжая при этом обеспечивать доступ клиентам по не-DFS каналу 36 по трем оставшимся радиоцепям. Если канал 104 чист, то ТД может отправить новое оповещение о переключении канала всем клиентам на канале 36, говоря им вернуться на исходный канал 104. Даже еще лучше, ТД может использовать одну радиоцепь MIMO, чтобы слушать другой DFS канал (например, канал 64). Если новый DFS канал чист в течении 60 секунд, то клиенты могут также на него перейти. Преимущество в том, что клиенты могут перейти на канал 64, а не ждать 30 минут, чтобы вернуться на канал 104.

**РИСУНОК 13.24** Симулятор импульсов радара WiFiMETRIX

Исторически, самой большой проблемой при использовании DFS каналов была потенциальное ошибочно-положительное обнаружение радара. Другими словами, ТД неправильно трактовали ложную радиопередачу как радар, и начинали изменение каналов, даже если им не нужно было его менять. Хорошая новость в том, что большинство производителей корпоративных БЛВС стали намного лучше в устраниении ошибочно-положительном обнаружении.

Как недавно говорилось, использование DFS каналов всегда рекомендовано кроме случаев, когда критичные для работы клиенты не поддерживают их. Если рядом присутствует радар, просто устраните влияние DFS каналов из 5ГГц канального плана.



#### Где я могу узнать больше о Динамическом Выборе Частоты?

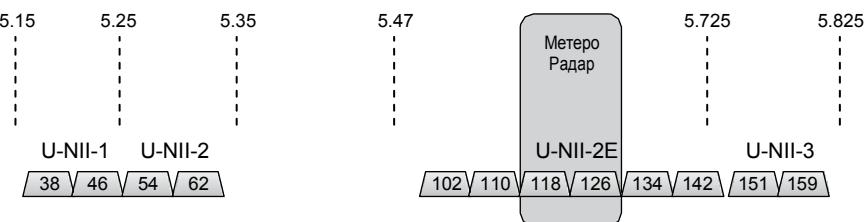
Если вам интересно узнать больше о DFS, лучшее место для старта – это просмотр этой видео презентации: “DFS – Нерассказанная История” [“DFS – The Untold Story”]: <http://bit.ly/DFS-video>. Соавтор этой книги, Дэвид Коулмен, провел эту лекцию в Феврале 2020 года на конференции WLANPros в Фениксе, Аризона. «Белый лист» [white paper] от NTS с названием “Динамический Выбор Частоты и 5 ГГц Безлицензионная Полоса” [ “Dynamic Frequency Selection and the 5 GHz Unlicensed Band”] является хорошим обзором общемировых регуляторных требований DFS, и доступен на [www.nts.com](http://www.nts.com).

## Планирование Канала 40МГц

Технология 802.11n представила возможность объединения двух 20МГц каналов, чтобы создать больший 40 МГц канал. Как вы узнали из Главы 10 "Технология MIMO: НТ и VHT" объединение каналов фактически удваивает полосу частот, что означает удвоение скорости передачи данных, которое может быть доступно на радиомодулях 802.11n/ac. Объединение каналов [channel bonding] также доступно для более новых радиомодулей 802.11ax.

Как показано на Рисунке 13.25, всего доступно двенадцать 40МГц каналов к использованию в 5 ГГц модели переиспользования, при развертывании корпоративной БЛВС, в зависимости от региона.

**РИСУНОК 13.25** 40 МГц каналы



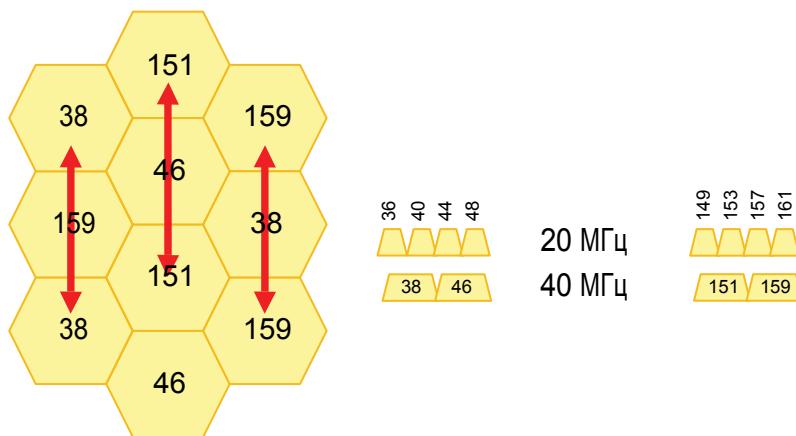
Итак, какие преимущества и недостатки использования объединения каналов [channel bonding] и 40 МГц каналов? На первый взгляд, вы можете подумать, что объединение каналов должно быть всегда включено из-за более высоких скоростей передачи данных, доступных на радиомодулях 802.11n/ac. Например, самая высокая потенциальная скорость передачи данных для радиомодуля 802.11n 3x3:3 MIMO это 217 Мбит/с. Самая высокая потенциальная скорость передачи данных для радиомодуля 802.11n 3x3:3 MIMO, передающего на 40 МГц канале - 450 Мбит/с. После взгляда на эти цифры, большинство администраторов посчитают, что объединение каналов должно быть включено по-умолчанию. Однако, многие производители точек доступа БЛВС требуют, чтобы объединение каналов включалось вручную, потому что существует потенциальный риск, что объединение каналов негативно ударит по производительности БЛВС.

Давайте вернёмся на один момент на 20 МГц дизайн. Преимущество использования 5 ГГц вместо 2,4 ГГц в том, что намного больше 20 МГц каналов в 5ГГц, которые могут быть использованы в модели переиспользования. Только три 20 МГц канала могут быть использованы в 2,4 ГГц. Проблема с использованием только трех 20 МГц каналов в том, что всегда будет существовать некоторая одноканальная интерференция, даже если они неперекрывающиеся. Следовательно, определенное количество избыточной служебной информации (оверхед) при борьбе за среду всегда присутствует в 2,4 ГГц просто потому, что недостаточно каналов и частотного пространства. Избыточная служебная информация при борьбе за среду на тех же самых 20 МГц каналах может быть почти полностью устранены в 5 ГГц, потому что больше каналов. 5 ГГц план переиспользования восьми или более 20 МГц каналов значительно уменьшит одноканальную интерференцию и избыточную служебную информацию (оверхед) при борьбе за среду.

Как изображено на Рисунке 13.26, рассматривайте 40 МГц модель переиспользования, используя только не-DFS каналы в U-NII-1 и U-NII-3 полосах. Если доступно только восемь 20 МГц каналов, то существует четырехканальная модель переиспользования 40МГц каналов. Хотя ширина полосы удвоена для радиомодулей 802.11n/ac/ax, увеличится избыточная служебная информация (оверхед) при борьбе за среду из-за того, что

есть только четыре 40 МГц канала, и точки доступа и клиенты на том же 40 МГц канале вероятнее всего будут слышать друг друга. Избыточная служебная информация (оверхед) при борьбе за среду может негативно повлиять и нивелировать любое увеличение в производительности, которое может предоставить расширенная полоса.

**РИСУНОК 13.26** Переиспользование 40 МГц каналов - четыре канала



Другая проблема с объединением каналов в том, что это обычно приводит к более высокому уровню шума примерно на 3 дБ. Если уровень шума на 3 дБ выше, то SNR (отношение сигнал-шум) на 3дБ ниже, что значит, что радиомодули могут перейти на более низкие скорости MCS, и следовательно более низкие модуляции скоростей передачи данных. Во многих случаях, это нивелирует некоторое увеличение полосы, которое предоставляет 40 МГц частотное пространство.

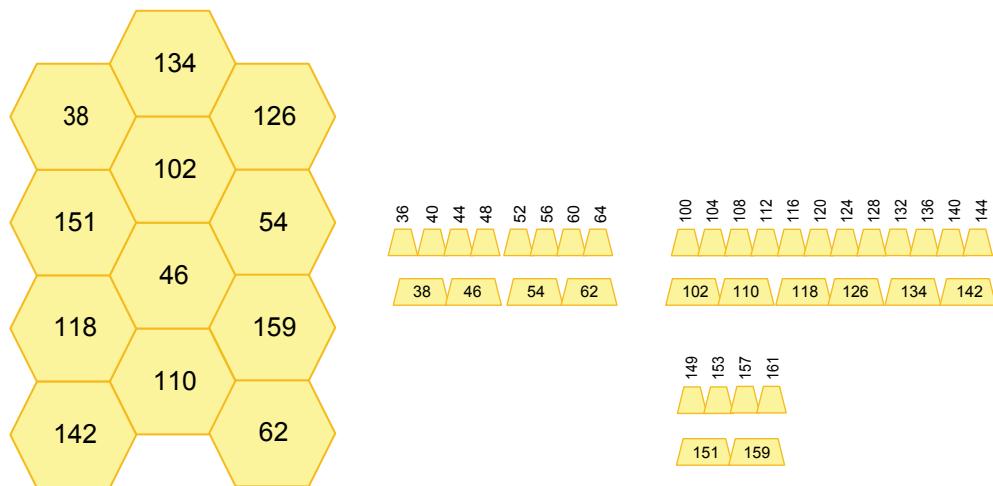
Итак, должны ли вы использовать объединение каналов или нет? Если доступно четыре или меньше 40 МГц каналов, то возможно вы не захотите включать объединение каналов, особенно, если 5 ГГц радиомодули передают на повышенном уровне мощности. Если основная часть клиентов БЛВС не поддерживает объединение каналов [channel bonding], то нет причины по включению этой возможности. Например, ранние версии смартфонов и планшетов с 802.11n не поддерживали объединение. Даже если все клиенты поддерживают 40 МГц объединение каналов, настойчиво рекомендуется протестировать производительность, если используются только четыре 40МГц канала.

Однако, если включена полоса DFS, то будет доступно больше 40МГц каналов; следовательно, будет доступна более лучшая модель переиспользования , которая уменьшает борьбу за среду. Загвостка в том, что клиентские радиомодули должны поддерживать DFS и должны поддерживать объединение каналов. Рисунок 13.27 изображает модель переиспользования 40 МГц каналов из 12 каналов, включая DFS-каналы. В этом примере, CCI меньше, потому что больше каналов.

Многие профессионалы БЛВС рекомендуют использовать 20 МГц каналы, а не 40 МГц каналы, в большинстве проектов БЛВС в 5 ГГц. Однако, сеть с 40 МГц каналами может работать с некоторым тщательным планированием и соблюдением нескольких общих правил:

- Использование четырех или меньше 40 МГц каналов в модели переиспользования будет недостаточным. Используйте 40 МГц каналы только, если доступны DFS каналы. Включение DFS каналов обеспечивает больше частотного пространства и следовательно больше доступных 40 МГц каналов для модели переиспользования.

**РИСУНОК 13.27** Переиспользование 40 МГц каналов—12 каналов



- Радиомодули ТД не должны передавать на полной мощности. Уровни мощности передачи в 12 дБм или ниже, обычно, более чем достаточны в большинстве сред в помещениях.
- Стены должны быть из плотного материала для затухания и уменьшения ССИ. Шлакобlockные, кирпичные или бетонные стены ослабят сигнал на 10 дБ и больше. Гипсокартон, однако, ослабит сигнал только на примерно 3 дБ.
- Если установка происходит в многоэтажной среде, рассмотрите отказ от использования 40 МГц каналов, пока нет значительного затухания сигнала между этажами.

Как вы узнали из Главы 10, 802.11ac представил возможность 80 МГц и даже 160 МГц каналов в полосе 5 ГГц. И хотя каналы 80 МГц и 160 МГц доступны в радиомодулях 802.11ac, они не должны использоваться на предприятии. Применение каналов 80 МГц и 160 МГц не масштабируется в БЛВС предприятия, потому что не достаточно частотного пространства. Уровни производительности значительно упадут, если 80 МГц каналы развернуты на нескольких ТД. 80 МГц канал должен быть использован только на одной ТД на изолированной области, такой как дом в сельской местности.

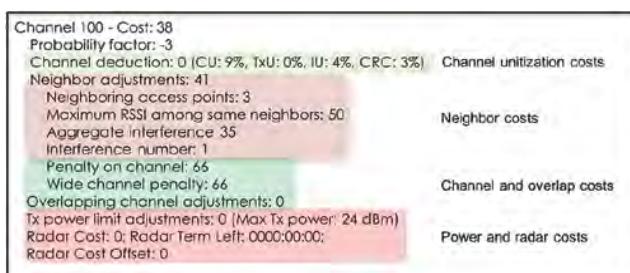
## Статические Каналы и Мощность Передачи против Адаптивного Радио

Вероятно самая обсуждаемая тема когда приходится проектировать Wi-Fi это использовать ли статические каналы и настройки мощности для ТД или же использовать адаптивные каналы и настройки мощности. Управление радио ресурсами [*Radio resource management (RRM)*] - это стандартный термин в индустрии, используемый для описания автоматической и адаптивной настройки мощности и канала точек доступа. ТД производителя БЛВС могут динамически изменять свою конфигурацию на основе накопленной информации о радио, собранной с радиомодулей точек доступа. Точки доступа подстраивают свои настройки мощности и канала, адаптивно изменения зону радиопокрытия на основе собранной информации о радиообстановке.

Управление радио ресурсами [Radio resource management] также называется адаптивным радио [*adaptive RF*]. Когда оно внедрено, RRM обеспечивает автоматическое изменение размера зоны и автоматический мониторинг и оптимизацию радиосреды, что может быть более точно описано как самоорганизующаяся беспроводная ЛВС. У большинства протоколов RRM также есть способность фиксации [*lockdown*], когда каналы и мощности автоматически были присвоены между ТД. Некоторые протоколы RRM также учитывают клиентские данные 802.11k, собранные с ассоциированных клиентов, которые поддерживают 802.11k.

Механизмы RRM, по большей части, являются проприетарными, и каждый производитель БЛВС использует свои эксклюзивные протоколы для возможностей адаптивного радио [*adaptive RF*]. Дополнительно, каждый производитель БЛВС будет вероятно использовать уникальное маркетинговое название технологии адаптивного радио. RRM, фактически, механизм плоскости контроля. Решение сделать адаптивные изменения в настройках канала и мощности ТД может быть распределено между точками доступа или может быть централизовано в контроллере БЛВС или облачной системе управления. Еще раз, у каждого производителя БЛВС есть свой собственный протокол адаптивного радио; однако, автоматическое назначение настроек канала и мощности основано на многочисленных весах [*costs*], определенных RRM алгоритмами производителя. Рисунок 13.28 показывает вычисления RRM весов одного из производителей БЛВС.

**РИСУНОК 13.28** Вычисление веса[cost] адаптивного радио.



Технология RRM получила широкое признание, потому что почти все производители БЛВС предлагают определенный тип решения адаптивного радио. Многие заказчики производителей имеют исключительный успех с установками с адаптивным радио. Предупреждаем, что торговые представители различных БЛВС заявляют, что проектирование БЛВС больше не требуется, из-за динамической и самоорганизующейся природы их RRM решений. Хотя технология адаптивного радио прошла длинный путь в последние годы, позволяя ТД адаптироваться к окружающей среде, RRM во всех смыслах не заменяет надлежащего проектирования БЛВС. Ручное обследование и/или обследование предиктивной модели должно быть первым делом перед развертыванием. После установки, должна быть выполнена соответствующая проверка проекта Wi-Fi сети. В Главе 14 вы узнаете о важности проверочного обследования. После развертывания, возможности адаптивного радио часто используются для изменения канала и мощности в живой работающей среде.

Как ранее упоминалось, использование RRM против проекта статического канала и мощности часто является очень горячо обсуждаемой. Много профессионалов БЛВС старой школы предпочитают вручную настраивать все каналы и мощности ТД, а не полагаться на адаптивные протоколы. Другие профессионалы предпочитают использовать исключительно RRM. Так должны ли вы использовать RRM или работать со статическими настройками? Ответ действительно зависит от предпочтений и опыта профессионала БЛВС и типа БЛВС дизайна.

Возможности Адаптивного радио включены по умолчанию на большинстве ТД каждого производителя БЛВС. Алгоритмы RRM постоянно улучшаются из года в год. Основная часть коммерческих заказчиков БЛВС используют RRM, потому что так проще разворачивать сеть. RRM обычно является предпочитаемым методом в корпоративных инсталляциях с тысячами ТД. Однако, следует уделить особое внимание использованию статических настроек канала и мощности в сложных радио средах. Большинство производителей БЛВС рекомендуют в своих собственных руководствах по установкам очень высокой плотности, чтобы использовались статические мощности и каналы, особенно когда устанавливаются направленные антенны.

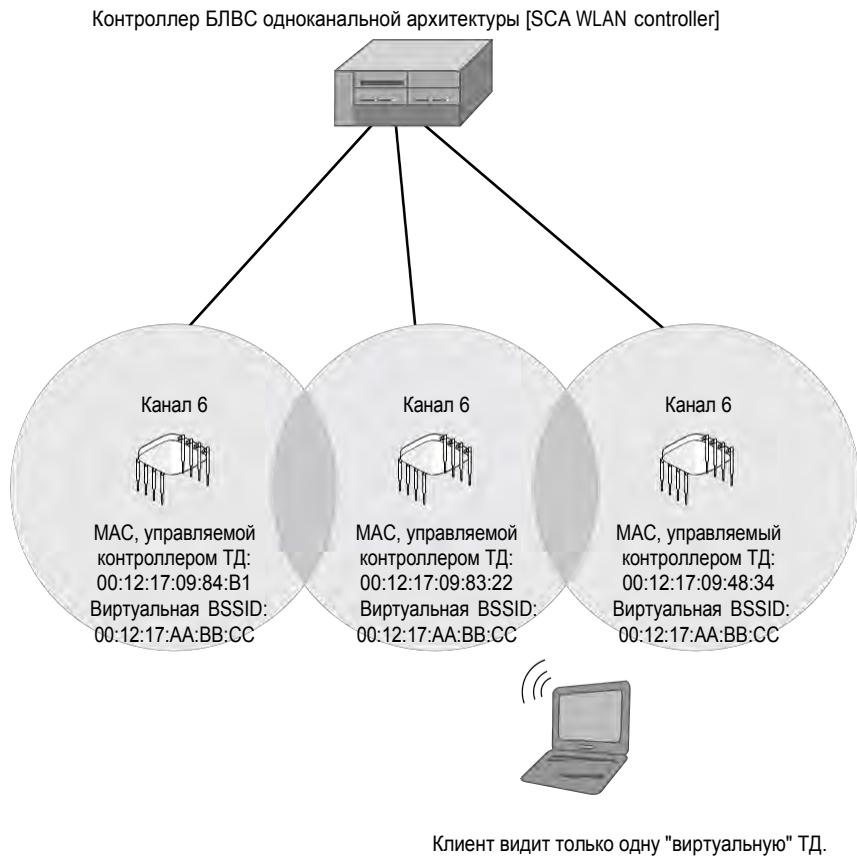
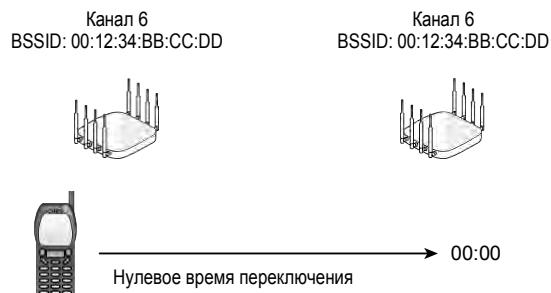
Мы не собираемся обсуждать за и против RRM против статической конфигурации в этой книге. Попробуйте думать об адаптивном радио [adaptive RF] как об еще одном инструменте в вашем арсенале по развертыванию БЛВС. У вас всегда есть возможность вручную установить настройки канала и мощности каждой ТД. Какой бы метод не был выбран, хорошо продуманный проект БЛВС и контрольное обследование всегда будут обязательным требованием.

## Одноканальная Архитектура

В прошлом, три производителя БЛВС — Fortinet, Allied Telesis, и Ubiquiti Networks — предлагали альтернативную конфигурацию для решения по планированию каналов БЛВС, называемую одноканальная архитектура [single-channel architecture (SCA)]. Представьте сеть БЛВС с несколькими точками доступа, передающими на одном и том же канале и использующих один и тот же BSSID. Одноканальная архитектура - это ровно то, что вы только что представили. Клиентские станции видят передачи на единственном канале с одним SSID (логическим идентификатором БЛВС) и одним BSSID (идентификатором на 2ом уровне). С точки зрения клиентской станции, есть только одна точка доступа. В этом типе архитектуры БЛВС, все точки доступа в сети могут быть развернуты на одном канале в 2,4 ГГц или 5 ГГц полосах частот. Восходящая и нисходящая передачи на едином канале 802.11 координируются контроллером БЛВС таким образом, что влияние одноканальной интерференции минимизировано.

Давайте сначала обсудим единый BSSID. Одноканальная архитектура состоит из контроллера БЛВС и нескольких точек доступа, управляемых контроллером. Как показано на Рисунке 13.29, у каждой ТД есть свой собственный радиомодуль со своим собственным MAC адресом; однако, они все используют *виртуальный BSSID* [*virtual BSSID*], который вещается на все точки доступа. Так как несколько точек доступа сообщают только один виртуальный MAC адрес (BSSID), клиентские станции полагают, что они подключены только к одной точке доступа, хотя они могут переключаться по нескольким физическим ТД. Вы знаете, что решения о роуминге (о переключениях) принимают клиенты. В системах одноканальной архитектуры (SCA) клиенты думают, что они ассоциированы только с одной ТД, таким образом они никогда не начинают роуминговый обмен на 2ом уровне. Все роуминговые переключения с точки на точку [*handoffs*] управляются центральным контроллером БЛВС.

Как показывает Рисунок 13.30, основное преимущество в том, что клиенты испытывают *нулевое время переключения* [*zero handoff time*], и проблемы с задержками, связанные с временем роуминга, решены. *Виртуальная ТД* [*virtual AP*], используемая решениями SCA, является потенциально превосходным решением для телефонов VoWiFi и решений 802.1X/EAP. Как мы обсуждали раньше, среднее время, затрачиваемое во время процесса аутентификации EAP, может быть 700 миллисекунд или больше. Каждый раз, когда клиентская станция переключается на новую точку доступа, требуется переаутентификация, когда развернуто решение по безопасности 802.1X/EAP. VoWiFi требует роуминговое

**РИСУНОК 13.29** Одноканальная архитектура**РИСУНОК 13.30** Нулевое время переключения [Zero handoff time]

Channel 6

переключение с точки на точку 150мс или меньше. Виртуальный BSSID устраняет необходимость переаутентификации при физическом переключении в одноканальной архитектуре. Клиент не начинает обмен сообщениями по переассоциации [reassociation exchange]—то есть , нулевое время переключения [zero handoff time].

Вы уже знаете, что клиентские станции принимают решения о роуминге в среде многоканальной архитектуры (MCA). Однако, клиентские станции не знают, что они переключаются (осуществляют роуминг) в среде одноканальной архитектуры (SCA). Клиенты должны все еще быть мобильными и поддерживать связь 2ого уровня между физическими точками доступа. Теперь все механизмы клиентского-роуминга управляются снова контроллером БЛВС, а решения о роуминге с клиентской стороны убраны. Все ассоциации станции управляются контроллером БЛВС одноканальной архитектуры (SCA), и контроллер SCA управляет всеми ТД. Контроллер SCA назначает уникальную точку доступа ответственной за управление нисходящей[downlink] передачей для индивидуальной клиентской станции. Когда контроллер получает входящую передачу клиента, SCA контроллер оценивает значения RSSI клиентской передачи. На основе измерений RSSI, контроллер SCA может зарезервировать определенную ТД для нисходящей передачи. Клиент полагает, что он ассоциирован с одной ТД. Однако, клиент перемещается между разными физическими ТД, на основе измерений RSSI, оцененных контроллером.

Одно большое преимущество одноканальной архитектуры в том, что больше нет проблем с интерференцией смежных каналов. Если все точки доступа работают на одном канале, то не может быть пересечения по частотам, и следовательно, нет интерференции смежных каналов. Однако, законный вопрос о решении БЛВС одноканальной архитектуры [SCA WLAN]: Почему не происходит одноканальной интерференции, если все ТД на одном и том же канале? Ответ в том, что одноканальная интерференция все еще существует, однако, контроллер БЛВС пытается централизованно управлять расписанием передач точек доступа, находящихся в зонах действия друг друга. Если все ТД на одном и том же канале в беспроводной сети многоканальной архитектуры (MCA), то появляется ненужная служебная информация [overhead] при борьбе за среду. В типовой среде MCA, каждая точка доступа имеет уникальный BSSID и отдельный канал, а зона покрытия каждой ТД является одним доменом коллизий. В беспроводной среде одноканальной архитектуры (SCA), домены коллизий управляются динамически контроллером SCA, на основе алгоритмов RSSI. Контроллер гарантирует, что близко находящиеся устройства не передают в одно и то же время. Большинство механизмов, используемых производителями SCA являются проприетарными, и находятся за пределами этой книги.

Многие годы, только что описанные процедуры были конкурентным преимуществом компаний, у которых есть SCA, при продаже по вертикалям рынка, где нужен был VoWiFi. Однако, с более широким принятием механизмов QoS, определенных WMM, и механизмов быстрого безопасного роуминга, определенного Голосовой связью уровня Предприятия [Voice-Enterprise], VoWiFi теперь активно разворачивается в более традиционной архитектуре MCA. Главные компании, у которых есть SCA, также предлагают возможность выключить SCA и использовать несколько каналов, как и все другие производители. Совершенно новые установки одноканальной архитектуры (SCA) теперь крайне редки; однако, вы можете найти такие модели сетей в старых инсталляциях.

Главный недостаток одноканальной архитектуры - проблема с емкостью, потому что доступен только один канал. В установке SCA в 2,4 ГГц, несколько ТД могут быть размещены в одном месте [co-located], используя три канала и три виртуальных BSSID. Проект размещения в одном месте [Co-location design] в одноканальной архитектуре часто называется *канальное наслаждение [channel layering]*. Каждый слой нескольких ТД, работающих на одном канале и использующих тот же самый BSSID, называется *канальное*

*покрытие [channel blanket]* или *канальный охват [channel span]*. Хотя это может звучать как теоретически хорошая идея, однако большинство заказчиков не желают платить за три размещенных вместе точки доступа везде, где требуется покрытие. Еще один возможный недостаток с архитектурой SCA в том, что домен борьбы за среду может быть очень большим. Хотя передачи ТД координируются контроллером SCA для минимизации коллизий с другими ТД, некоторые реализации технологии SCA могут быть высоко проприетарными, и нет гарантии, что клиентские передачи могут быть безуказненно контролируемыми.

Как недавно упоминалось, дизайны SCA можно все еще найти в старых инсталляциях БЛВС, которые используют эту технологию. Однако, SCA считается устаревшей технологией и поддержка SCA приостанавливается у трех производителей, которые сначала предлагали это проприетарное использование канала.

## Планирование Емкости

При проектировании беспроводной сети обычно соперничают друг с другом две концепции емкость [*capacity*] и дальность [*range*]. На заре беспроводных сетей было обычным установка точки доступа с мощностью, установленной на максимальный уровень, чтобы обеспечить насколько возможно большую площадь покрытия. Обычно это было приемлемо, потому что было мало беспроводных устройств. Также, точки доступа были очень дорогие, поэтому компании пытались обеспечить большее покрытие используя меньше точек доступа.

Распространенный вопрос, который часто задается: “Какая дальность зоны действия ТД?” В теории, радиосигнал будет путешествовать всегда в свободном пространстве; однако, правильный ответ в том, что “фактическая” дальность ТД в действительности зависит от затухания в среде местонахождения. Более важно, что эффективная зона действия ТД должна рассматриваться с точки зрения клиента. Другими словами, дальность — это не просто клиентское подключение, но также и производительность клиента. Фактическая зона действия [Effective range] означает, что клиентские устройства могут эффективно переключаться (осуществлять роуминг) и могут взаимодействовать с ТД вместе с другими клиентами, используя высокие скорости передачи данных.

С быстрым увеличением беспроводных устройств сетевой дизайн радикально изменился по сравнению с тем каким он был вначале. Теперь БЛВС редко проектируются строго с точки зрения дальности и покрытия. Вместо этого, большинство БЛВС проектируются в основном фокусируясь на требованиях клиентской емкости. Это не значит, что покрытие теперь игнорируется. Вы все еще должны планировать принимаемый сигнал на –70 дБм (или сильнее), высокое SNR, бесшовный роуминг, и надлежащую модель переиспользования каналов. Собственно говоря, то как вы спроектируете покрытие также повлияет на требования по емкости. Как недавно упоминалось, ТД, настроенные на передачу на полной мощности больше не являются идеалом. Три ТД, передающие на 100мВт могут обеспечить покрытие с –70 дБм на территории в 929 квадратных метрах (10 000 квадратных футов), но что, если 1000 или более клиентским устройствам нужен Wi-Fi доступ на этой самой площади? Полоса БЛВС, которую эти три ТД могут обеспечить, даже близко не соответствует требованиям по клиентской емкости.

Настройка мощности передачи ТД для ограничения фактической зоны покрытия называется *регулировкой размера соты* [*cell sizing*] и является одним из наиболее типовых способов по выполнению требований по клиентской емкости. Типовые инсталляции БЛВС внутри помещений проектируются с ТД, настроенными от одной четвертой до одной трети мощности передачи. Среды с более высокой плотностью пользователей и клиентов могут требовать, чтобы мощность передачи ТД была установлена на самую минимальную настройку в 1 мВт. Другими словами, нужно больше ТД, чтобы удовлетворить требованиям по емкости, и, следовательно, мощность передачи ТД нужно будет уменьшать. Ограничение мощности передачи ТД также помогает уменьшить одноканальную интерференцию (CCI), вызванную ТД, которые имеют прямое влияние на производительность. БЛВС с высокой пользовательской и клиентской плотностью становится большей проблемой из-за произошедшего взрывного роста клиентских устройств. Wi-Fi сети больше не только для беспроводного подключения ноутбуков. Большинство пользователей теперь хотят подключиться к корпоративной БЛВС с нескольких

устройств, включая планшеты и смартфоны с радиомодулями Wi-Fi. К счастью, технологии 802.11n/ac/ax предоставляют большую полосу и эффективность по обращению с большим количеством клиентов; однако, даже точки доступа 802.11n/ac/ax могут стать перегруженными без надлежащего планирования емкости.

## Высокая Плотность

Термин *высокая плотность [high-density (HD)]* и *очень высокая плотность [very high-density (VHD)]* часто используются при обсуждении проектирования емкости и планирования БЛВС. Разные инженеры БЛВС имеют разные мнения относительно того что составляет БЛВС высокой плотности; однако, из-за изобилия клиентских устройств большинство БЛВС нужно считать с высокой плотностью по умолчанию. Чтобы внести некоторую ясность в терминологию, БЛВС высокой плотности могут обычно описываться тремя различными сценариями:

**Высокая Плотность [High-Density]** Почти все БЛВС являются средами с высокой плотностью из-за широкого распространения многочисленных пользователей с несколькими устройствами. Среднестатистический человек может хотеть подключиться к корпоративной БЛВС тремя или четырьмя Wi-Fi устройствами. Очевидно, что плотность клиентских устройств также зависит от числа пользователей. Большинство сред высокой плотности состоит из нескольких территорий, где роуминг также является верхним приоритетом. ТД установлены во множестве разных кабинетов со стенами, которые часто вносят разные уровни затуханий.

**Очень Высокая Плотность [Very High-Density]** Любая среда БЛВС, у которой есть огромное количество людей на одном открытом пространстве, часто называется как БЛВС очень высокой плотности (VHD). Основные примеры включают аудитории, спортивные залы, кафетерии и т.д. В большинстве сред VHD нет стен, которые вносят затухание. Все ТД скорее всего слышат друг друга на открытом пространстве. Дизайн БЛВС очень высокой плотности является совершенно сложным и отличается от стандартной среды высокой плотности со стенами. Как обсуждается позже в этой главе, среда VHD обычно требует установку направленных антенн, для обеспечения секторов покрытия.

**Ультра Высокая Плотность [Ultra High-Density]** БЛВС ультра высокой плотности [ultra high-density (UHD)] определен как среда с десятками тысяч пользователей и устройств на одном и том же пространстве. Лучшие примеры БЛВС ультра высокой плотности это стадионы и спортивные арены. Проектирование этих типов сред требует бывальных профессионалов БЛВС с опытом в проектировании Wi-Fi на стадионах.

Древний вопрос, который заказчики БЛВС всегда задают: Сколько клиентских устройств может подключиться к радиомодулю ТД? Корректный ответ - по-разному. Никто не любит этот ответ, но просто существует очень много переменных, чтобы всегда давать один и тот же ответ для точки доступа любого производителя БЛВС. Заводские настройки радиомодуля корпоративного БЛВС могут позволять 100-250 клиентских подключений. Поскольку большинство корпоративных ТД двухчастотные с радиомодулями 2,4 ГГц и 5ГГц, то теоретически 200-500 клиентов может быть ассоциировано с радиомодулями одной ТД. Хотя более 100 устройств может подключиться к радиомодулю ТД, это число не реалистично для активных устройств из-за природы полудуплексной общей среды. Требования по производительности этого множества клиентских устройств не будут удовлетворены и пользовательский опыт будет печальным. Ощущение будет что Wi-Fi “медленный”.

Если точка доступа использует радиомодули 802.11n/ac с 20МГц каналами, то хорошее эмпирическое правило в том, что каждый радиомодуль может поддерживать 35-50 активных устройств для среднестатистического использования, такого как просмотр веб-страниц и проверка электронной почты. Однако, числа могут значительно варьироваться, на основе широкого разнообразия переменных. Следующие, вероятно три самых больших вопроса, которые нужно задать:

**Какой тип приложений будет использоваться в БЛВС?** Как недавно утверждалось, 35-50 активных Wi-Fi устройств на радиомодуль, работающих через двух-частотную точку доступа 802.11n/ac, и использующих среднестатистическое приложение, такое как просмотр веб-страниц и электронной почты, является реалистичным. Однако, приложения с интенсивным использованием полосы, такие как потоковое видео высокой четкости [high-definition video streaming], окажут сильное влияние. Различные приложения требуют разную пропускную способность TCP, как показано в Таблице 13.2.

**ТАБЛИЦА 13.2** Приложения и Потребление Пропускной способности TCP

Приложение	Требуемая Пропускная Способность
Email/просмотр веб страниц	от 500 кбит/с до 1 Мбит/с
Печать на принтере	1 Мбит/с
Потоковое SD видео	от 1 Мбит/с до 1,5 Мбит/с
Потоковое HD видео	от 2 Мбит/с до 5 Мбит/с

**Сколько ожидается пользователей и устройств?** Три важных вопроса нужно будет задать относительно пользователей. Первый, скольким пользователям на текущий момент нужен беспроводной доступ, сколько Wi-Fi устройств они будут использовать? Второй, скольким пользователям и устройствам может понадобиться беспроводной доступ в будущем? Эти первые два вопроса помогут вам начать планировать адекватно хорошее отношение количества устройств на точку доступа, позволяя при этом расти в будущем. Третий вопрос огромного значения – где находятся пользователи? Садитесь с администраторами сети и обозначьте на поэтажном плане здания все области с высокой плотностью пользователей. Например, у одной компании могут быть офисы с одним или двумя сотрудниками на кабинет, в то время как у другой компании может быть 30 или более людей на общей территории разделенной кубическими перегородками. Другие примеры областей с высокой плотностью пользователей – это колл центры, классы, и лекционные залы. Вы должны всегда планировать проведение контрольного радиообследования с присутствием пользователей, а не в нерабочие часы. Высокая концентрация человеческих тел может уменьшить радиосигнал за счет поглощения.

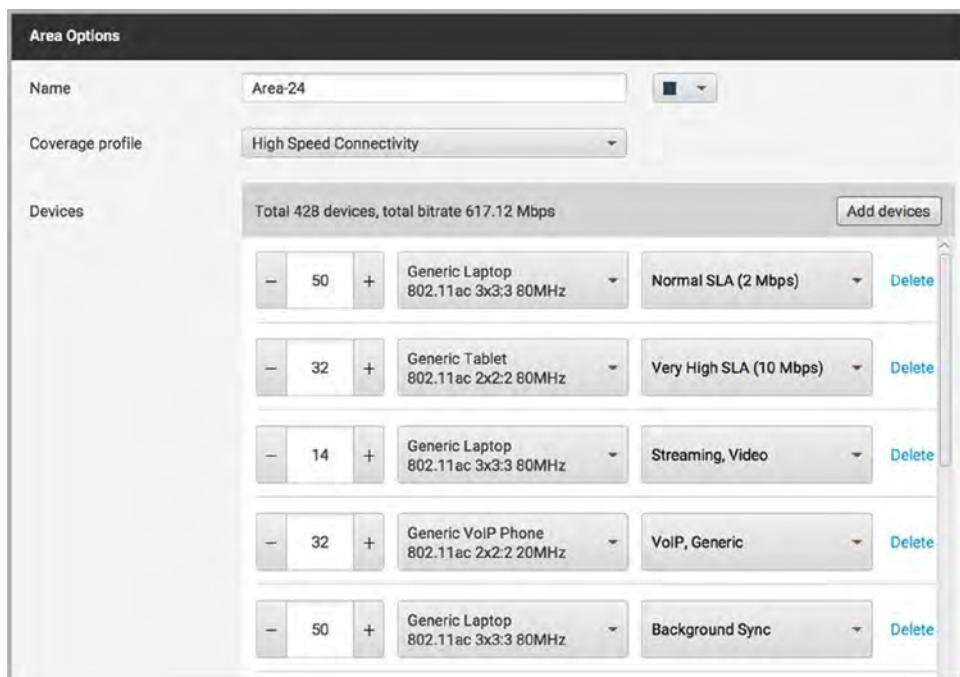
**Какой тип клиентских устройств подключается к БЛВС?** Всегда помните, что все клиентские устройства не одинаковы. Много клиентских устройств потребляют больше эфирного времени [airtime] из-за меньших возможностей MIMO. Например, старые планшеты 802.11n с радиомодулем 1×1:1 MIMO передающие на 20 МГц канале могут достичь скорости передачи данных в 65 Мбит/с с пропускной способностью TCP от 30 Мбит/с до 40 Мбит/с. Планшет 802.11n с

радиомодулем 2×2:2 MIMO, передающим на 20МГц канале, может достичь скорости передачи данных в 130 Мбит/с с пропускной способностью TCP от 60 Мбит/с до 70 Мбит/с. У многих ноутбуков также есть возможности 3×3:3 MIMO и таким образом они способны на более высокие скорости передачи данных. Большинство новых смартфонов и планшетов сейчас поддерживают 2×2:2 MIMO.

Дело в том, что устройства с меньшими возможностями MIMO потребляют больше эфирного времени [airtime], и, следовательно, негативно влияют на агрегированную производительность любой БЛВС. ТД может эффективно обслужить больше клиентов 2×2:2 MIMO по сравнению с устаревшими клиентами 1×1:1 MIMO, которые работают на меньших скоростях передачи данных. Разворачивание сетей на предприятиях почти всегда будут требовать некоторый уровень обратной совместимости для обеспечения доступа старых радиомодулей 802.11a/b/g, находящихся в ручных устройствах, VoWiFi телефонах, или старых ноутбуках.

Некоторые из коммерческих инструментов предиктивного моделирования БЛВС, такие как Ekahau Site Survey, позволяют вам обозначить определенные области с высокой плотностью на этажном плане здания. Как показано на Рисунке 13.31, внутри каждой области вы можете определить количество устройств, типы устройств, и какой трафик приложений ожидается. Алгоритмы моделирующего программного обеспечения подстроят размещение ТД, мощности и настройки канала на основе этих переменных при этом продолжая удовлетворять требования по покрытию.

После того как вы определили типы устройств, которые будут использоваться, и типы приложений, вы можете рассчитать количество потребления эфирного времени. Например, Apple iPad, передающий на 20 МГц канале, может подключиться на скорости передачи данных 65 Мбит/с и может достичь максимум 30 Мбит/с пропускной способности TCP. 2 Мбит/с видео приложение, работающее на iPad будет занимать 6,67 процентов эфирного времени 20 МГц канала ( $2 \text{ Мбит/с} \div 30 \text{ Мбит/с} = 6.67\%$ ). Ноутбук с 2×2:2 MIMO, передающий на 20 МГц канале, может подключиться со скоростью передачи данных в 130 Мбит/с и может достичь максимум пропускной способности TCP близко к 70 Мбит/с. То же самое 2Мбит/с HD видео приложение, работающее на ноутбуке, будет занимать около 2,86 процента эфирного времени [airtime] ( $2 \text{ Мбит/с} \div 70 \text{ Мбит/с} = 2.86\%$ ).

**РИСУНОК 13.31** Предиктивное моделирование плотности

После того, как вы определили количество потребления эфирного времени [airtime], вы можете вычислить количество активных устройств, которое радиомодуль ТД может поддерживать. Wi-Fi эксперт Эндрю фон Наги [Andrew von Nagy], CWNE #84, рекомендует несколько хороших формул для этих вычислений. Точка доступа 802.11 считается полностью загруженной при 80 процентах утилизации эфирного времени. Чтобы оценить число поддерживаемых устройств на одном радиомодуле ТД, разделите индивидуальное эфирное время, требуемое каждому устройству, на 80 процентов:

$$80 \div \text{потребление эфирного времени одного устройства} = \# \text{ устройств на радиомодуль ТД}$$

Например, 2Мбит/с приложение HD видео, работающее на iPad'ах потребляет 6,67 процентов эфирного времени на устройство. Следовательно,  $80 \div 6.67 = 12$  iPad'ов, которые могут выполнять приложение конкурентно на 20 МГц канале через один радиомодуль ТД 802.11n/ac. Вероятнее всего, ТД имеет 2,4 ГГц и 5 ГГц радиомодуль; следовательно, на 24 iPad может работать одно и то же приложение HD видео через одну ТД, если устройства были сбалансированы по двум частотам. То же самое 2Мбит/с приложение HD видео, работающее на ноутбуке, потребляет 2,86 процента эфирного времени на устройство. Следовательно,  $80 \div 2.86 = 28$  ноутбуков, которые могут предположительно выполнять приложение конкурентно на 20 МГц канале через один радиомодуль ТД 802.11n/ac.

Чтобы вычислить нужное число радиомодулей ТД, умножьте число клиентских устройств на процент потребления эфирного времени, и затем разделить на 80 процентов:

$$(\# \text{ устройств} \times \% \text{ потребления эфирного времени одного устройства}) \div 80\% = \text{число радиомодулей ТД}$$

Например,  $(150 \text{ iPads} \times 6.67\%) \div 80\% = 12.5$  радиомодулей ТД. Следовательно, семь двухдиапазонных ТД могут адекватно обслуживать 150 iPadов конкурентно, которые конкурентно используют приложения с очень высокой полосой. Что, если вам также нужно 150 ноутбуков, использующих тоже самое потоковое(стриминговое) приложение на той же самой территории с iPadами? Вычислим  $(150 \text{ ноутбуков} \times 2.86\%) \div 80\% = 5.36$  радиомодулей ТД. Следовательно, вам вероятно понадобится еще три двухдиапазонных точки доступа. Итого 10 двух-диапазонных ТД 802.11n, передающих на 20 МГц каналах на 150 iPadах и 150 ноутбуках.



Вас не будут проверять на знание этих формул на экзамене CWNA-108. Держите в уме, что эти числа являются оценочными, и берут в рассмотрение оба радиомодуля ТД. Расширенное тестирование после развертывания – это всегда хорошая идея.

## Сколько ТД на Комнату?

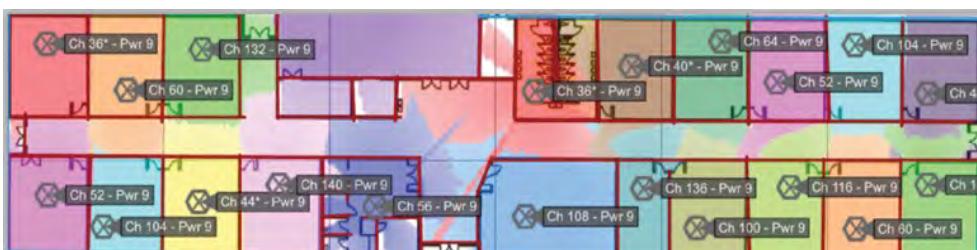
Местоположение, где физически смонтированы ТД также нужно брать во внимание, опираясь на требования по емкости. На некоторых больших площадях зданий могут находиться только один, или два, или три пользователя, которым требуется Wi-Fi доступ. Наоборот, на других пространствах, таких как аудитории, могут быть сотни пользователей, которым нужно Wi-Fi соединение.

Во многих вертикалях, таких как 12 летнее школьное обучение, из-за требований к емкости, стало обычным устанавливать одну ТД на класс. Обратите внимание, что одна ТД на класс (12 летнего обучения) может также быть совершенно не нужна. Одной ТД на каждые два или три класса может быть достаточно, чтобы удовлетворить требования по емкости.

Сколько ТД нужно зависят от требований к емкости и соглашением с заказчиком. Нужно вам установить одну ТД в каждый класс? Еще раз, это зависит от числа устройств, типов устройств, и трафика приложений. Однако, в среднем 70 или более Wi-Fi устройств на класс стало преобладающим в большинстве образовательных сред. Как показано на Рисунке 13.32, с соответствующим размещением ТД, низкой мощностью передачи, и переиспользованием каналов, установка одной ТД на класс, с использованием 5 ГГц радиомодуля является подходящей. Мощность передачи 5 ГГц радиомодуля обычно 9дБм (8мВт) или меньше, и 20 МГц каналы являются рекомендованными в большинстве случаев.

Стены должны быть сделаны из толстого материала, такого как бетон или кирпич, в целях затухания и помощи ограничения одноканальной интерференции (ССГ).

**РИСУНОК 13.32** Одна ТД на класс—5 ГГц



Вы заметите в Рисунке 13.32, что всего установлено 20 ТД, использующих план переиспользования 5 ГГц каналов для предотвращения одноканальной интерференции (CCI). Большинство ТД являются двух диапазонными и у них есть 2,4 ГГц радиомодуль. Так как существует только три канала, и из-за непосредственной близости этих 20 ТД, большая часть радиомодулей 2,4 ГГц ТД должны быть выключены, чтобы помочь минимизировать одноканальную интерференцию (CCI). В установках с высокой плотностью, становится очень распространенным выключать два из трех или даже три из четырех 2,4 ГГц радиомодуля в двух-частотных ТД. В большинстве случаев, три из четырех 2,4 ГГц радиомодулей будет более чем достаточно, чтобы обеспечить необходимое покрытие для 2,4 ГГц в том же самом пространстве, где двадцать 5 ГГц радиомодулей обеспечивают основную массу требований по емкости. Большинство производителей БЛВС применяют собственную балансировку нагрузки, управление полосой и другие механизмы MAC уровня для большей помощи в требованиях по емкости в среде с высокой плотностью пользователей. При правильном планировании клиентской емкости необходимо тщательно продумать, какие клиенты и сколько клиентов подключаются к полосе 2,4 ГГц, а сколько подключаются к полосе 5 ГГц. Также нужно учесть балансировку нагрузки клиентов между полосами частот и между индивидуальными ТД.

## Управление Выбором Полосы

Безлицензионный 5 ГГц частотный спектр предлагает много преимуществ в сравнении с безлицензионным частотным спектром 2,4ГГц для Wi-Fi связи. 5ГГц полосы U-NII предоставляют более широкий диапазон частотного пространства и намного больше каналов.

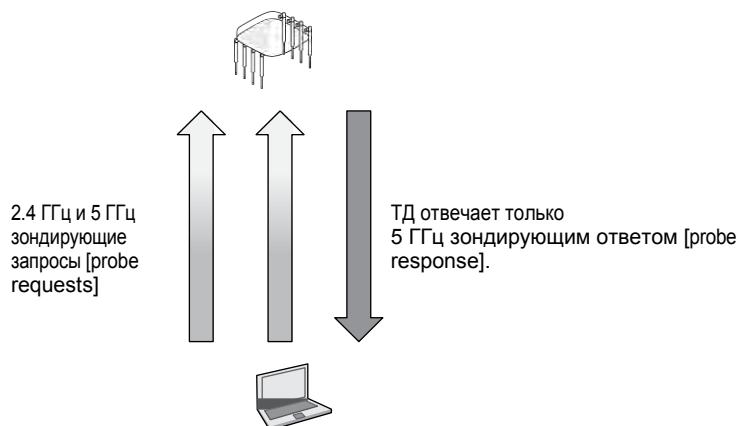
Правильная модель переиспользования 5 ГГц каналов, использующая несколько каналов, значительно уменьшает избыточную служебную информацию(оверхед) при борьбе за среду, вызванную одноканальной интерференцией [co-channel interference]. В полосе 2,4 ГГц всегда присутствует избыточная служебная информация при борьбе за среду из-за одноканальной интерференции (CCI) просто потому, что существует только три канала.

Еще одна основная губительная особенность полосы 2,4 ГГц в том, что в дополнение к работе сетей Wi-Fi, полоса интенсивно используется многими другими типами устройств, включая микроволновые печи, радионяни, беспроводные телефоны, и видеокамеры. Со всеми этими устройствами, работающими в том же самом частотном диапазоне, намного больше радио интерференции и намного выше уровень шума, чем в полосах 5 ГГц.

Итак, если использование 5 ГГц полос предоставит лучшую пропускную способность и производительность, то как мы можем сподвигнуть Wi-Fi клиентов использовать эту полосу? Для тех кто только начал, это клиент решает к какой ТД и в какой полосе подключиться, обычно на основе более сильного сигнала, который он слышит для анонсируемого SSID. Большинство точек доступа имеют оба радиомодуля и 2,4ГГц и 5 ГГц, с них обоих осуществляется широкое вещание одних и тех же SSID. Поскольку 5 ГГц сигналы по природе затухают сильнее, чем сигнал 2,4 ГГц, то клиентский радиомодуль вероятнее всего определит, что радиомодуль 2,4 ГГц имеет более сильный сигнал и подключится к ней по умолчанию. Во множестве сред, клиент будет способен выполнить быстрое качественное подключение с любым радиомодулем ТД, но выберет сигнал 2,4 ГГц, потому что он сильнее. Технология, которая называется *управление выбором полосы(диапазона)* [*band steering*], может сподвигнуть двух-полосные клиентские радиомодули подключиться к 5 ГГц радиомодулю ТД, вместо 2,4 ГГц радиомодуля ТД.

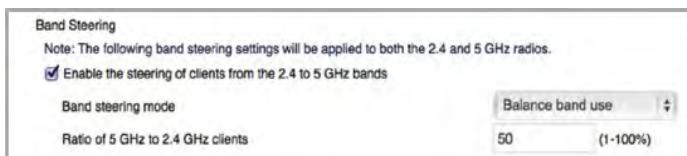
Управление выбором полосы [Band steering] - это технология разработанная не IEEE 802.11. На момент этого написания, все реализации управления выбором полосы являются проприетарными. Хотя реализации управления выбора полосы являются проприетарными, большинство производителей применяют эту технологию, используя похожие техники манипуляции с MAC под уровнем. Когда двух-частотный клиент стартует первый раз, он передаст зондирующий запрос [probe requests] на обоих полосах 2,4 ГГц и 5 ГГц, в поисках ТД. Когда двухчастотная ТД слышит зондирующий запрос [probe requests] на обеих полосах, исходящий от одного и того же клиента, то ТД знает, что клиент может работать в полосе 5 ГГц. Как изображено на Рисунке 13.33, ТД попробует направить клиента в 5 ГГц полосу, отвечая клиенту с использованием только 5 ГГц передачи. Хотя клиент направлен на 5 ГГц радиомодуль ТД, могут быть причины для клиента, чтобы подключиться к ТД, используя радиомодуль 2,4 ГГц. Если клиентский радиомодуль продолжает пытаться подключиться к ТД, используя полосу 2,4 ГГц, ТД в конце концов разрешит подключение.

**РИСУНОК 13.33 Управление выбором полосы на 5 ГГц**



Хотя управление выбором полосы обычно используется для мотивации клиента для подключения к 5 ГГц точкам доступа, клиенты также могут быть направлены в полосу 2,4 ГГц. Как показано на Рисунке 13.34, многие производители БЛВС могут определить процент клиентов для направления в 5 ГГц полосу, а остальное направить в полосу 2,4 ГГц. В средах, где присутствует высокая плотность клиентских устройств, управление выбором полосы на обе частоты может быть использовано для балансировки на почти одинаковое число клиентов по обоим радиомодулям ТД. Например, 55 клиентов подключено к радиомодулю 2,4 ГГц, и 60 клиентов подключено к радиомодулю 5 ГГц. Фактически, управление выбором полосы может быть использовано для балансировки нагрузки клиентов между двумя частотами. Пожалуйста, не перепутайте этот тип балансировки частот одной ТД с балансировкой нагрузки клиентов между несколькими точками доступа. Балансировка нагрузки между несколькими точками доступа описана в следующем разделе этой главы.

**РИСУНОК 13.34** Управление выбором полосы для балансировки по частотам



У клиентов обычно намного лучшее соединение и лучшая производительность, когда они подключены к 5 ГГц полосе, вот почему производители ТД предлагают возможности управления выбором полосы. Итак, должно ли быть включено управление выбором полосы на двухчастотной ТД? Хорошо, еще раз, правильный ответ – по-разному. Большинство устаревших клиентских устройств, у которых есть двухчастотный функционал, будут предпочитать полосу 2,4 ГГц, и управление переключением полосы на 5 ГГц может быть необходимо. Однако, во множестве новых клиентских устройств реализован проприетарный выбор полосы с клиентской стороны. Например, клиентские устройства macOS и iOS обычно предпочитают подключаться к радиомодулю 5 ГГц ТД до их ассоциации с радиомодулем 2,4 ГГц ТД. Некоторые производители клиентов также предпочитают возможность настройки предпочтений по полосе с клиентской стороны с помощью программных клиентских утилит.

Прежде чем включать управление выбором полосы на ваших ТД, вы можете захотеть промониторить каков процент ваших клиентских устройств ассоциирован с радиомодулем 5 ГГц. Если большая часть устройств все еще предпочитает 2,4 ГГц, то управление выбором полосы в сторону 5 ГГц вероятно является хорошей идеей. Держите в голове, что у многих устаревших клиентов есть только радиомодули 2,4 ГГц, а они не могут подключиться к 5 ГГц радиомодулям. У многих устройств IoT также только радиомодуль 2,4 ГГц и у них нет возможностей 5 ГГц. Лучшая стратегия в терминах проектирования БЛВС – это обеспечение покрытия 2,4 ГГц специально для устаревших устройств и устройств IoT.

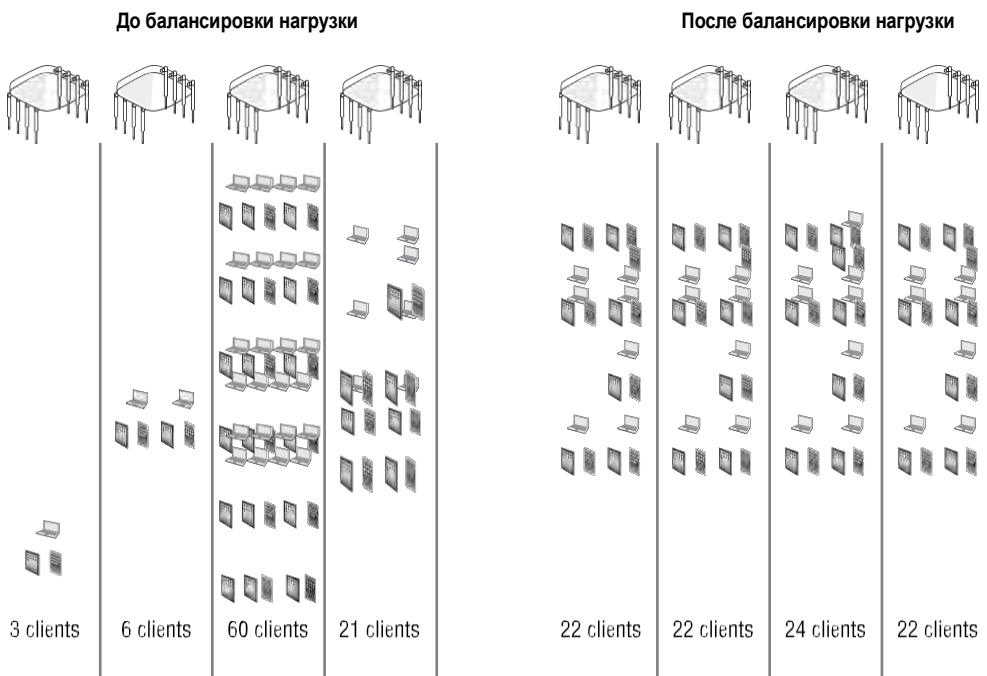
На предприятии, полоса 2,4 ГГц часто считается «негарантированной» [ “best effort”] полосой частот, а 5 ГГц каналы зарезервированы для всех других клиентов, которым требуются более высокие метрики производительности. Еще одна стратегия, иногда используемая для сегментации устройств между двумя полосами частот, это сегментация (или разделение) SSID [SSID segmentation]. Другими словами, критичные SSID вещаются только на 5 ГГц полосе. Например, создайте один SSID с названием *ACME-2.4* и еще один SSID с названием *ACME-5*. На клиентской стороне настройте SSID профили: *ACME-2.4* для IoT устройств и старых устаревших устройств, у которых есть только 2,4 ГГц радиомодуль. Для критичных для бизнеса устройств, которые могут

поддерживать обе полосы, создайте профили на клиентской стороне для SSID *ACME-5*. Это гарантирует, что более чистая полоса 5 ГГц используется для более новых устройств и также предотвращает роуминг между полосами частот, которое может часто быть разрушительным для пользовательского опыта с Wi-Fi.

## Балансировка Нагрузки

Производители БЛВС также используют методы по манипуляции MAC подуровнем, чтобы балансировать клиентов между несколькими точками доступа. Как проиллюстрировано на Рисунке 13.35, балансировка клиентской нагрузки между точками доступа гарантирует, что одна ТД не перегружена слишком большим количеством клиентов, и все клиентские устройства могут быть обслужены многочисленными ТД, в итоге давая более лучшую производительность. Когда клиент хочет подключиться к ТД, клиент отправит кадр запроса на ассоциацию [association request frame] к ТД. Если ТД уже перегружена слишком многими клиентами, то ТД отложит ответ на запрос на ассоциацию [association response] клиенту. Надежда в том, что клиент затем отправит еще один запрос на ассоциацию другой ближайшей ТД с меньшей клиентской нагрузкой. Спустя время, клиентские ассоциации будут честно сбалансированы по нескольким ТД. Информация о клиентской нагрузке будет очевидно распространена между точками доступа. Балансировка нагрузки – это механизм плоскости контроля, который присутствует и в распределенной архитектуре, где все ТД общаются друг с другом, используя проприетарный протокол, и в централизованной архитектуре, которая использует контроллер БЛВС.

**РИСУНОК 13.35** Балансировка нагрузки между ТД



### Когда должна быть включена балансировка клиентской нагрузки между ТД?

Предупреждаем, что включение возможностей балансировки нагрузки производителей БЛВС должно быть сделано только при определенных условиях. Балансировка нагрузки между точками доступа обычно применяется на территориях, где очень высокая плотность клиентов и роуминг не обязательно в приоритете—например, спортивный зал или аудитория с 20 установленными ТД на одной открытой территории. В этой среде, клиент будет скорее всего слышать все 20 ТД, и балансировка нагрузки между ТД обычно является необходимой.

Однако, на территориях, где необходим роуминг, балансировка нагрузки – нехорошая идея, потому что механизмы могут стать причиной, что клиенты станут «залипшими» и останутся ассоциированными с ТД на очень долго. Если кадры ответов на ассоциацию и переассоциацию от ТД отложены, клиентская мобильность вероятнее всего сломается. Поймите, что балансировка нагрузки между ТД может быть губительной для процесса роуминга.

## Потребление Эфирного Времени

С годами, грандиозный взрыв клиентский Wi-Fi устройств совместно с улучшенными технологиями 802.11 заставили нас переобдумать как мы проектируем БЛВС.

Проектирование с точки зрения количества клиентских устройств теперь стало нормой.

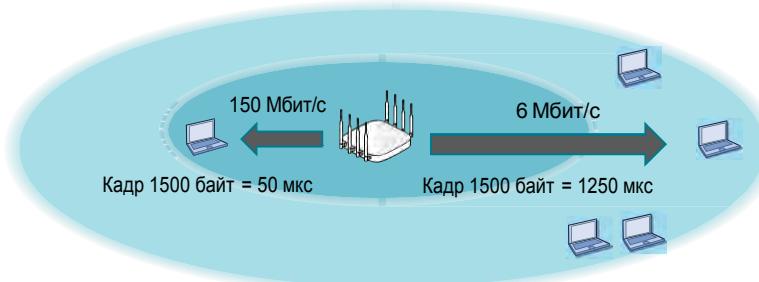
Лучшие практики БЛВС теперь диктуют, чтобы вы проектировали так, чтобы минимизировать *потребление эфирного времени* [*airtime consumption*], которое напрямую связано с планированием емкости. На протяжении всей этой книги, вы узнали, что Wi-Fi - это полудуплексная радиосреда, и только один радиомодуль может передавать на канале в любое выбранное время. Когда бы ни выиграл радиомодуль возможность передачи [*transmission opportunity*] (TXOP), радиомодуль монополизирует доступное эфирное время до тех пор, пока он не закончит передачу. Да, каждому радиомодулю нужно быть способным передать и доставить данные; однако, существует несколько простых лучших практических советов проектирования БЛВС, которые минимизируют ненужное потребление эфирного времени.

Одноканальная интерференция является высшей причиной бесполезной траты эфирного времени, которое может быть минимизировано с надлежащими лучшими практическими советами по дизайну БЛВС, как описано ранее в этой главе. Проектирование покрытия на уровне –70 дБм и высоким отношением сигнал-шум (SNR) также гарантирует, что клиентские устройства будут передавать кадры данных 802.11 на высоких скоростях передачи данных, на базе возможностей клиентского радиомодуля. Итак, какие еще лучшие практические советы по проектированию БЛВС, которые могут уменьшить потребление эфирного времени?

Один из лучших способов срезать потребление эфирного времени – это выключить некоторые низкие скорости передачи данных на ТД. Рисунок 13.36 изображает ТД, взаимодействующую с несколькими клиентскими станциями на 6 Мбит/с, при этом работая с одним единственным клиентом с использованием скорости передачи данных 150 Мбит/с. Когда радиомодули 802.11 передают на очень низких скоростях передачи данных, например 6 Мбит/с или даже меньше, они фактически вызывают излишнюю служебную информацию (оверхед) при борьбе за среду для передатчиков с более высокими скоростями передачи данных из-за долгого времени ожидания. Радиомодуль, передающий 1500 байтный кадр данных на 150 Мбит/с может занимать среду на 50 микросекунд. А радиомодуль,

передающий на 6 Мбит/с, может занять 1250 микросекунд для доставки тех же самых 1500 байт. Другими словами, одна и также полезная нагрузка потребляет эфирного времени на 2500 процентов больше, когда доставляется на низкой скорости передачи данных.

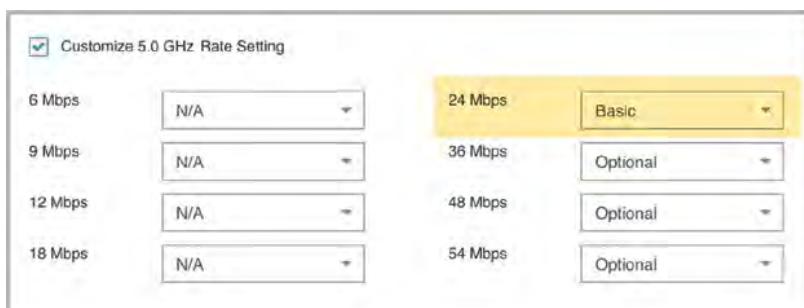
Ранее в этой главе, вы узнали о динамическом переключении скоростей, которое позволяет радиомодулям ТД и клиентам переключаться между скоростями передачи данных по мере того как клиент удаляется от ТД. Клиенты и ТД, которые переключаются на низкие скорости передачи данных потребляют больше эфирного времени и негативно влияют на общую

**РИСУНОК 13.36** Время передачи кадра

производительность БЛВС. Вместо переключения клиента на более низкие скорости передачи данных, лучший сценарий будет для клиента – переключиться на другую ТД с сильным сигналом и продолжить соединение с высокой скоростью передачи данных. Надлежащее проектирование роуминга с первичным и вторичным покрытием должны решать этот вопрос.

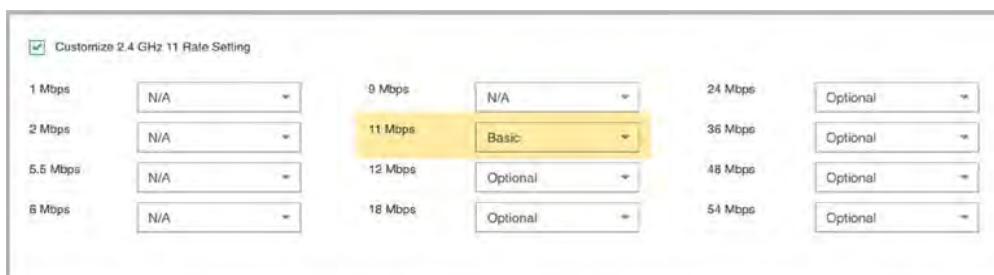
Еще более важная причина, чтобы отключить низкие скорости передачи данных, – это уменьшение потребления эфирного времени кадрами управления и контроля 802.11. В Главе 9 вы узнали, что для того, чтобы клиентская станция успешно ассоциировалась с ТД, клиент должен быть способен общаться на любых настроенных базовых скоростях [*basic rates*], которые требует ТД. Базовые скорости, настроенные на ТД, считаются “обязательными” скоростями для всех радиомодулей, работающих в BSS. Нужно понимать, что ТД будет передавать все кадры управления и много контрольных кадров на самой низкой настроенной базовой скорости. Кадры данных могут быть переданы с на много большими поддерживаемыми скоростями передачи данных.

Например, радиомодуль 5 ГГц ТД будет передавать все кадры маяки и другой трафик контроля и управления на 6Мбит/с, если базовая скорость радиомодуля настроена на эту скорость. Это потребляет огромное количество эфирного времени. Следовательно, обычная практика – это настроить базовую скорость [*basic rate*] радиомодуля 5 ГГц на ТД или на 12Мбит/с, или даже на 24 Мбит/с, как показано на Рисунке 13.37. Не настраивайте базовую скорость радиомодуля ТД на 18 Мбит/с, потому что некоторые клиентские драйверы могут быть не способны разобрать ее. Потребление эфирного времени кадров управления, переданных на 24 Мбит/с, на 400 процентов меньше, чем, переданных на 6 Мбит/с.

**РИСУНОК 13.37** Базовые скорости – 5 ГГц

Тоже самое может быть сказано для настройки базовых скоростей для любого радиомодуля 2,4 ГГц ТД. Базовая скорость или 12 Мбит/с, или даже еще лучше, 24 Мбит/с будет потреблять значительно меньше эфирного времени для трафика управления 802.11. Однако, устаревшие клиенты 802.11b будут не способны подключиться. Это не обязательно плохая вещь. Технологии 802.11b уже больше 20 лет, и в идеале все клиенты 802.11b были заменены или убраны много лет назад. В реальном мире, однако, это не всегда так. Если требуется подключения радиомодуля-динозавра 802.11b, то базовая скорость 2,4 ГГц должна быть 11Мбит/с, как показано на Рисунке 13.38. Лучшим практическим советом будет устранение всех радиомодулей 802.11b из состава эксплуатируемого оборудования, и выключение всех скоростей HR-DSSS в 1, 2, 5.5, и 11 Мбит/с на точке доступа. И аналогично на 5 ГГц, выключить скорости OFDM в 6 и 9 Мбит/с, и назначить 12 Мбит/с в качестве базовой скорости передачи данных для радиомодуля 2,4 ГГц точки доступа.

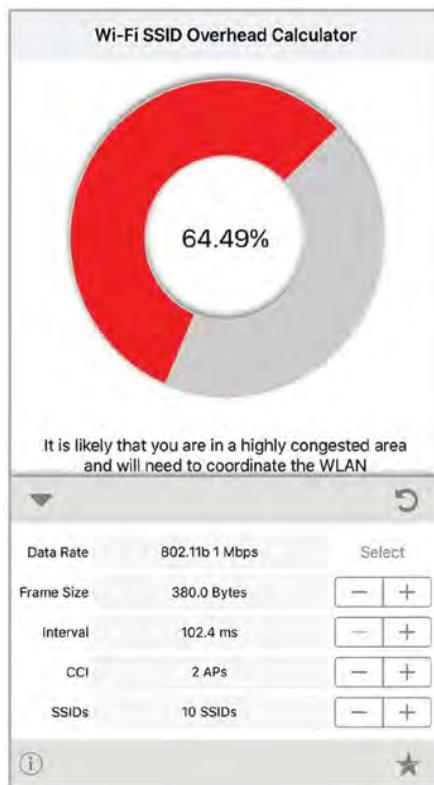
**РИСУНОК 13.38** Базовые скорости – 2,4 ГГц



Выключение низких скоростей передачи данных и назначение высоких скоростей передачи данных для базовой скорости уменьшит потребление эфирного времени. Как описано в Главе 15, побочный эффект такого дизайна БЛВС в увеличении проблем “залипших” роуминговых клиентов и проблем скрытых узлов.

Еще один лучший практический совет по проектированию БЛВС – это уменьшить число передаваемых SSID на ТД. Большинство производителей БЛВС предлагает возможность передачи до 16 SSID на радиомодуль. Проблема в том, что когда ТД настроена на несколько SSID, ТД будет передавать кадры маяки для каждого SSID. Когда клиентские станции отправляют кадры зондирующего запроса [probe request], ТД будет также отвечать несколькими кадрами ответов на зондирующий запрос[probe response]. Последствия избыточной служебной информации (оверхед) потребления эфирного времени при передачи нескольких маяков и зондирующих ответов [probe response] значительны. В ранние дни проектирования БЛВС, несколько SSID были нужны и соответствовали уникальным пользовательским VLANам и IP подсетям, чтобы сегментировать трафик. Как вы узнаете из Главы 17 “802.11 Архитектура Сетевой Безопасности”, SSID могут быть консолидированы, чтобы помочь убрать избыточную служебную информацию (overhead). Пользователи могут быть ассоциированы с одним SSID и привязаны к разным VLANам, или им могут быть назначены другие политики доступа путем использования RADIUS атрибутов.

Стандартные лучше практические советы диктуют, чтобы вешалось не более 3-4 SSID. Как показано на Рисунке 13.39, калькулятор количества избыточной служебной информации SSID может помочь вам в определении потребления эфирного времени избыточными передачами маяков. Вы можете загрузить бесплатный калькулятор количества избыточной служебной информации по адресу <http://bit.ly/SSIDcalc>.



Авторы этой книги недавно посещали тренинг Сертифицированный Профессионал по Беспроводному Проектированию [Certified Wireless Design Professional (CWDP)], предлагаемый Divergent Dynamics (<https://divdyn.com>). Одно из упражнений во время обучения требовало от студентов придумать как можно больше уникальных способов по ограничению потребления эфирного времени. Лучшие практические советы по проектированию БЛВС, обсуждаемые на протяжении всей этой главы, были очевидно правильными ответами для упражнения. Однако, в зависимости от установки индивидуальной БЛВС, производитель БЛВС, и даже профессионал БЛВС может использовать много креативных способов по уменьшению потребления эфирного времени. Настройки конфигурации производителя БЛВС, такие как уменьшение зондов [probes], уменьшение широковещательного трафика, уменьшение IPv6 и изоляция клиентов, могут быть подходящими в конкретных средах БЛВС. Помните всегда, что эфирное время - это драгоценный товар. Любой метод, который может быть использован для уменьшения потребления эфирного времени, при этом обеспечивающий необходимую производительность БЛВС и мобильность, является горячо приветствуемым.

## Голос или Данные

Как вы уже знаете, большинство приложений по передаче данных в сети Wi-Fi могут работать со скоростью повторных передач на 2ом уровне до 10 процентов без заметной деградации в производительности.

Однако, приложения чувствительные ко времени, такие как VoIP, требуют, чтобы потери IP пакетов более высокого уровня были не более 2 процентов. Следовательно, сетям с Голосом поверх Wi-Fi [Voice over Wi-Fi (VoWiFi)] нужно ограничить повторные передачи на 2м уровне до 5 процентов или меньше, чтобы гарантировать своевременную и последовательную доставку VoIP пакетов. Когда повторные передачи на 2ом уровне превышают 5 процентов, могут развиться проблемы с задержкой, и скорее всего встанут проблемы с вариацией задержки (jitter). VoWiFi связь более чувствительна к повторным передачам на 2м уровне; следовательно, при проектировании БЛВС голосового уровня, сигнал в -65 дБм или сильнее является рекомендованным таким образом, чтобы получаемый сигнал был выше уровня шума.

Многие БЛВС изначально спроектированы, чтобы обеспечить покрытие только для приложений для передачи данных, а не для голоса. Даже в слабо спроектированной БЛВС, корпоративные приложения передачи данных могут продолжать работать, хоть и не оптимально. Многие компании решают добавить решение VoWiFi к своей БЛВС после исходной установки. Они быстро обнаруживают, что исходный дизайн БЛВС не был оптимизирован для голосовой связи. Телефоны VoWiFi могут иметь прерывистый звук или проблемы с эхом, а голосовой вызов может даже разъединиться. Добавление голоса в БЛВС часто выявляет существующие проблемы: Так как приложения передачи данных могут выдерживать намного большую скорость повторных передач на 2ом уровне, проблемы, которые существуют в БЛВС, могут оставаться незамеченными. Как показано в Таблице 13.3, голосовой IP трафик более чувствителен к задержкам или непоследовательной доставке пакетов из-за повторных передач на 2м уровне.

**ТАБЛИЦА 13.3** Сравнение IP Голоса и IP Данных

IP Голос	IP Данные
Небольшие, одинакового размера пакеты	Пакеты переменного размера
Равномерная, предсказуемая доставка	Взрывная доставка
Сильно подвержен влиянию задержек и непоследовательной доставке пакетов	Минимально подвержены влиянию задержек и непоследовательной доставке пакетов
“Лучше никогда, чем поздно”	“Лучше поздно, чем никогда”

Оптимизация БЛВС для поддержки голосового трафика оптимизирует сеть для всех беспроводных клиентов, включая клиентов, использующих приложения передачи данных, а не только голосовых. Надлежащий дизайн БЛВС и контрольное радио обследование уменьшат повторные передачи 2ого уровня и обеспечат среду с бесшовным покрытием, которое требуется для VoWiFi сетей. Все возможные причины повторных передач 2ого уровня обсуждаются далее подробно в Главе 15. Так как голос так чувствителен к негативному воздействию повторных передач 2ого уровня, настойчиво рекомендуется предлагать VoWiFi связь только в 5 ГГц полосе частот и вообще избегать 2,4 ГГц.

Хотя голосовой трафик обычно смешан с трафиком других приложений передачи данных,

которые проходят через ту же самую точку доступа, одна из стандартных практик – выделение голосового трафика в отдельный SSID. Голосовой SSID может настроить несколько параметров QoS и установок энергосбережения, чтобы оптимизировать голосовой трафик. Всегда консультируйтесь с производителем клиентов VoWiFi для выяснения рекомендованных настроек DTIM, U-APSD, и других настроек по-SSID.

Параметры Контроля Допуска WMM [WMM Admission Control] могут также быть настроены, чтобы указать число разрешенных активных звонков VoWiFi.



## Пример из Реальной Жизни

### Сколько вызовов VoWiFi может поддержать точка доступа?

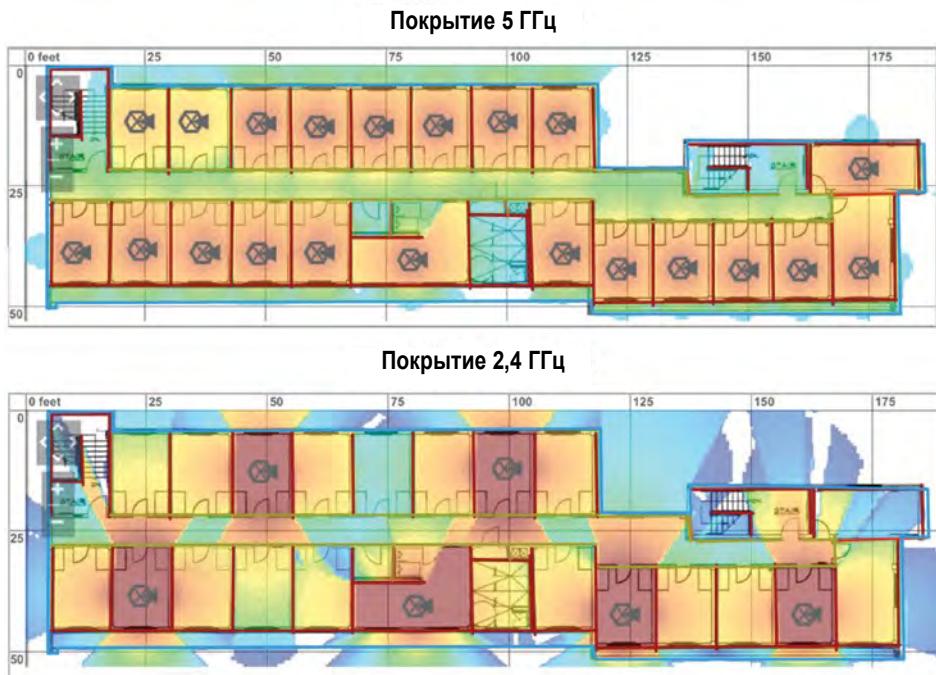
Несколько факторов вступают в игру, включая доступную полосу, средняя утилизация, и специфичные для производителя характеристики. При развертывании в 5 ГГц, Cisco, производитель БЛВС, рекомендует максимум 27 одновременных двунаправленных голосовых вызовов при подключении на 24 Мбит/с и выше. Из-за борьбы за среду, это рекомендованное число падает до 20 вызовов при подключении на 12 Мбит/с. Различные, характерные для определенного производителя, характеристики точки доступа могут также влиять на число конкурентных вызовов, и рекомендуется проводить расширенное тестирование. Также существуют вероятностные модели для прогнозирования трафика VoWiFi. Не каждый пользователь телефона VoWiFi будет осуществлять вызов в одно и то же время. Вероятностные формулы трафика используют телекоммуникационную единицу, называемую эрланг [*erlang*]. Эрланг равен одному часу телефонного трафика в течении одного часа времени. Некоторые онлайн калькуляторы эрлангов VoWiFi трафика могут быть найдены на [www.erlang.com](http://www.erlang.com).

# Два 5 ГГц радиомодуля и Программно-Определяемые радиомодули

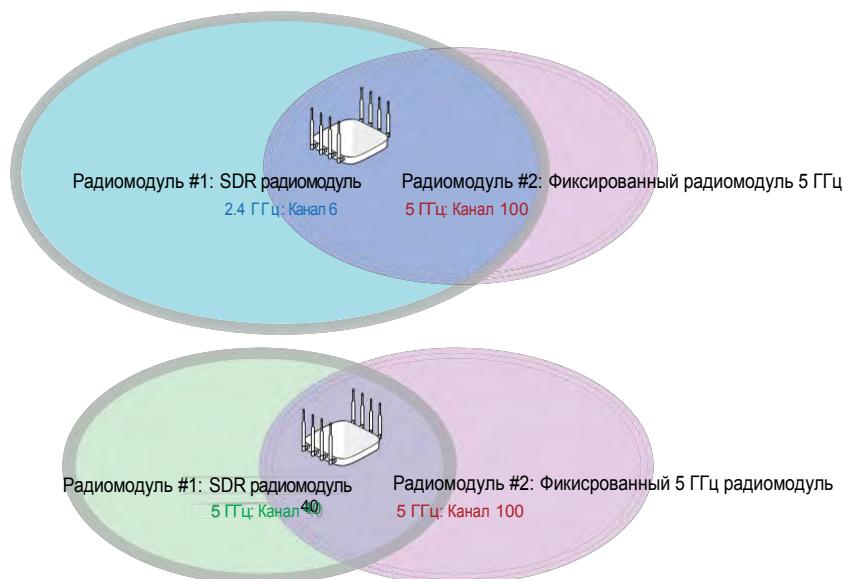
Ранее в этой главе вы узнали, что в проектах БЛВС высокой плотности выключение нескольких радиомодулей 2,4 ГГц в двухчастотных ТД часто является необходимым для ограничения одноканальной интерференции (CCI) в полосе 2,4 ГГц. Одна ТД может быть установлена на комнату для обеспечения покрытия 5 ГГц и удовлетворения потребности по емкости. Однако, 60-75 процентов 2,4 ГГц радиомодулей могут быть выключены, как показано на Рисунке 13.40. Большая часть 2,4 радиомодулей ТД должна быть выключена, чтобы помочь минимизировать CCI. В действительности, лучшим вариантом будет преобразование спящих радиомодулей 2,4 ГГц в сенсоры. У ТД уровня предприятия есть режим радио сенсора(датчика), который фактически разрешает радиомодулю быть только в состоянии радиопрослушивания. Радиомодули сенсоры полезны для задач триангуляции для обнаружения неучтенно [rogue] ТД, а также для сервисов местоположения клиентов, которые может предоставить производитель БЛВС. Как ранее упоминалось, производители корпоративных БЛВС используют адаптивные радио протоколы для назначения каналов и настроек мощности для радиомодулей ТД динамически. На основе радио условий некоторые из этих протоколов также могут автоматически выключать радиомодуль 2,4 ГГц. Еще раз, переключение радиомодуля 2,4 ГГц в режим сенсора является предпочтительным.

Более новая тенденция у производителей БЛВС – предлагать программно определяемый радиомодуль [*software-defined radio (SDR)*] вместе с фиксированным радиомодулем 5 ГГц в двух частотной ТД. Радиомодуль, у которого есть функциональность SDR, может работать как на 2,4 ГГц, так и на 5 ГГц. В результате, ТД с двумя радиомодулями (один фиксированный и один SDR) могут или предлагать покрытие в 2,4 ГГц и 5 ГГц, или предлагать покрытие на двух разных 5 ГГц каналах. Радиомодуль с функцией SDR иногда также называется *программно выбираемое radio [software selectable radio (SSR)]*. На примере, показанном на Рисунке 13.41, фиксированный 5ГГц радиомодуль настроен на канал 100. Радиомодуль с функциональностью SDR передает или на канале 6 в полосе 2,4 ГГц или на канале 40 в полосе 5 ГГц.

**РИСУНОК 13.40** Покрытие 2,4 ГГц vs. покрытие 5 ГГц



**РИСУНОК 13.41** Двойное 5 ГГц покрытие



Итак, какие, точно, преимущества и смысл для БЛВС в обеспечении *двойного 5 ГГц [dual 5 GHz]* покрытия от одной и той же ТД? Считаем, что в дизайне для высокой плотности, который мы обсудили, 60-75 процентов радиомодулей 2,4 ГГц отключено или преобразовано в сенсоры. Альтернативой может быть преобразование большей части этих 2,4 ГГц радиомодулей в 5ГГц радиомодули. Радиомодули SDR могут быть настроены, вручную или автоматически, для работы на 5 ГГц каналах. Например, предположим, что развернуто 20 ТД в здании с высокой плотностью пользователей. Все фиксированные 5ГГц радиомодули в 20 ТД включены и назначены определенным 5 ГГц каналам. Дополнительно, пять программно-определеных радиомодулей будут передавать на 2,4 ГГц каналах, а остальные 15 SDR будут обеспечивать покрытие на 5 ГГц каналах. Весь смысл в двойном 5ГГц покрытии – в предоставлении большей емкости. Радиомодуль 2.4 ГГц, который был выключен, не может обслуживать клиентов; однако, SDR, работая как дополнительный 5 ГГц радиомодуль, может обслуживать клиентов и предоставлять больше эфирного времени.

Хотя и превосходный для требований по емкости, двойной 5 ГГц дизайн БЛВС не без потенциальных проблем. Основная проблема в гарантировании того, что два радиомодуля в одной ТД не интерферируют друг с другом, когда оба радиомодуля ТД передают на 5 ГГц каналах. Все производители БЛВС для предприятий используют отдельные аппаратные и программные возможности так, что два радиомодуля 5 ГГц могут работать внутри одной и той же физической ТД. Некоторые производители используют дорогие полосовые [band-pass] фильтры для предотвращения интерференции внутри ТД. Другие производители используют технологии умных [smart] антенн с несколькими антенными элементами, создающими требуемый разнос радиосигналов между двумя одновременно работающими 5 ГГц радиомодулями. Одно постоянно – это то, что должно быть некоторое частотное разнесение между двумя передающими 5 ГГц радиомодулями в одной и той же ТД. Рекомендации производителя могут требовать где-то от 60 до 100 МГц разнесения по частотам между этими двумя 5 ГГц радиомодулями.

Независимо от того настроены ли радиомодули вручную или автоматически, нужно тщательное планирование каналов при двойном 5 ГГц планировании. Несмотря на то, что может вам сказать некоторая маркетинговая литература, используйте только 20 МГц каналы в двойном 5 ГГц дизайне. Использование 40 МГц каналов в двойном 5 ГГц дизайне обычно не рекомендуется, кроме некоторых крайних случаев. Так как вам нужно будет как можно больше 20 МГц каналов, то почти всегда требуется включение DFS каналов. Из-за требуемого канального разнесения внутри каждой ТД, нужно стратегия образования пар каналов, как показано в Таблице 13.4. Если возможно, образование пар не-DFS каналов с DFS каналами является хорошей стратегией, на случай когда некоторые устаревшие клиенты не поддерживают DFS.

**ТАБЛИЦА 13.4** Канальные Пары ТД с Двумя 5 ГГц радиомодулями.

ТД	Канальная Пара	ТД	Канальная Пара
ТД #1	36/100	ТД #5	149/116
ТД #2	40/104	ТД #6	153/132
ТД #3	44/108	ТД #7	157/136
ТД #4	48/112	ТД #8	161/140

Еще одна проблема, которую стоит опасаться при развертывании нескольких ТД с двумя 5 ГГц радиомодулями – это потенциальное увеличение одноканальной интерференции (CCI). Как ранее упоминалось, одно из преимуществ 5 ГГц в том, что модель переиспользования каналов обычно может убрать CCI, если доступны все каналы. Однако, поскольку удваивается число радиомодулей ТД, использующих 5 ГГц каналы, вероятность того, что ТД и клиенты могут услышать друг друга на одном и том же канале становится больше. Вы бы не захотели иметь ТД с парой каналов 36/100 с физически близко стоящей с другой ТД с парой 100/48. Радиомодули на канале 100 будут слышать друг друга и откладывать передачи. Как вы видите, планирование двойных 5ГГц каналов может быть сложным, и любой протокол RRM адаптивного радио также должен учитывать все эти переменные.

## Проектирование БЛВС 6 ГГц

Как вы узнали из Главы 6, ожидается, что все основные производители БЛВС для предприятий будут предлагать трех полосные Wi-Fi 6E точки доступа где-то с 2021 года. В первое время, эти ТД будут предоставлять Wi-Fi доступ в полосе частот 6 ГГц в дополнение к полосам 2,4 ГГц и 5 ГГц. Эти ТД вероятнее всего будут доступны в разнообразных форм факторах (корпусах), из-за конкурирующей природы сетевой индустрии. Таблица 13.5 отображает три возможных форм фактора корпоративных ТД Wi-Fi 6 E; однако, многие другие комбинации также найдут свой путь на рынок. Займет некоторое время когда провайдеры Автоматической Координации Частот [Automated Frequency Coordination (AFC)]

**ТАБЛИЦА 13.5** Возможные Формы Факторы ТД Wi-Fi 6E

Форм Фактор	Радиомодуль	Частота
ТД #1	2×2:2	2.4 ГГц
	2×2:2	5 ГГц
	2×2:2	6 ГГц
ТД #2	4×4:4	SDR: 2.4 ГГц или 5 ГГц
	4×4:4	5 ГГц
	4×4:4	6 ГГц
ТД #3	2×2:2	SDR: 2.4 ГГц или 5 ГГц
	4×4:4	5 ГГц
	4×4:4	6 ГГц
	2×2:2	Радиомодуль-сенсор

станут работать. Следовательно вам стоит ожидать, что внешние ТД Wi-Fi 6E задержатся с выходом на рынок, по сравнению с внутренними ТД.

Хотя исторически 1 Гбит/с каналов подключения [uplink] более чем достаточно, мы предсказываем, что по крайней мере каналы подключения [uplink] в 2,5 Гбит/с в итоге станут требоваться для предприятий. По мере роста количества клиентских Wi-Fi устройств, трафик, создаваемый по всем трем частотам, будет требовать много-гигабитных каналов подключения [uplink]. Хорошая новость в том, что все трех полосные радиомодули уровня предприятия станут стандартом с 2,5 или 5 Гбит/с проводными портами. Однако, коммутаторы уровня доступа может понадобится обновить. Коммутируемые порты с PoE Plus также будут требоваться для успешной подачи питания большинству трех-полосных ТД.

Так как 6 ГГц никогда не использовался до Wi-Fi связи, у профессионалов БЛВС появился новые вызовы и размышления при проектировании трех-полосного покрытия. Как упоминалось в Главе 6, один из немедленных примеров использования, ожидаемый для 6 ГГц Wi-Fi будет внутренний транзитный канал для взаимосвязности [mesh] внутри помещений. Устаревшие клиенты 2,4 ГГц и 5 ГГц будут подключаться к ТД для доступа, а 6 ГГц радиомодули в ТД будут использоваться для транзитных взаимосвязных каналов связи.

## Обзор клиентов

Ключевая разница для 6 ГГц частотной полосы с технологией 802.11ax в том, что не нужна обратная совместимость. Так как радиомодули 802.11a/b/g/n/ac работают только в полосах 2, 4 ГГц и 5 ГГц, и не работают в 6 ГГц полосе, то не нужны механизмы защиты RTS/CTS. Частотная полоса 6 ГГц будет “чистой” полосой технологии 802.11ax для Wi-Fi связи. В результате, будет меньше избыточной служебной информации (оверхед) MAC в кадрах управления. Информационные элементы специфичные не-802.11ax технологиям будут не нужны. Например, информационные элементы НГ (802.11n) и VHT (802.11ac) не будут использоваться в маяках и кадрах зондирующих ответов. Полоса 6 ГГц также является более чистым спектром без требований по динамическому выбору частоты для уклонения от радара. Однако, отсутствие обратной совместимости также означает, что существующие клиенты 2,4 ГГц и 5 ГГц никогда не подключаются в 6 ГГц, потому что у них нет функционала 6 ГГц.

Вам нужно держать в голове, что существующие клиенты 2,4 ГГц и 5 ГГц никуда не уйдут в ближайшее время. Пятнадцать миллиардов Wi-Fi клиентов на текущий момент не поддерживают 6 ГГц, и ни один из существующих клиентов не будет способен подключиться к 6 ГГц радиомодулю в ТД Wi-Fi 6E. Только клиенты Wi-Fi 6E с 6 ГГц радиомодулями будут способны связываться по 6 ГГц каналам. Клиенты с 6 ГГц возможностями не заполнят рынок мгновенно. Хотя корпоративные ТД могут иметь трех-пяти летний жизненный цикл, клиенты всегда отстают. Зайдет некоторое время пока клиенты 6 ГГц насытят рынок и найдут свой путь на предприятия.

Устаревшие клиентские устройства будут повсюду еще очень долгое время; следовательно, клиентский доступ на 2,4 ГГц и 5 ГГц будет оставаться приоритетным. Как ранее обсуждали, полоса 2,4 ГГц будет все еще считаться “негарантированной” [“best effort”] полосой частот, а 6 ГГц каналы будут использоваться для клиентов, которым требуются более высокие параметры производительности. Однако, потенциал 6 ГГц совершенно изумителен из-за всего нового доступного частотного пространства (1200 МГц). По мере роста количества устройств с 6 ГГц, БЛВС будут также проектироваться для покрытия 6 ГГц внутри помещений.

## Обзор Покрытия

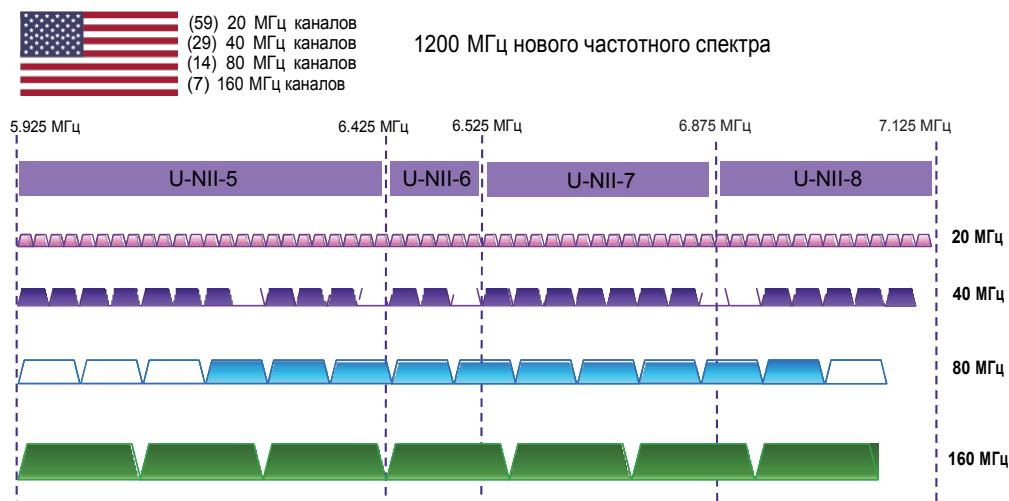
В прошлом, планирование покрытия было для двух полос. Для двух частотных ТД, планирование и подтверждение покрытия на  $-65$  дБм или  $-70$  дБм, проектирование основано на 5 ГГц покрытии. Причина в том, что фактическая зона обслуживания 5 ГГц обычно намного меньше, чем 2,4 ГГц. Следовательно, использование меньшего общего делителя 5 ГГц зоны предпочтительнее. Как ранее упоминалось, очень часто, многие радиомодули 2,4 ГГц отключают.

Для установок “с нуля” с трехполосными ТД, которые включают 6 ГГц радиомодули, наименьший общий знаменатель будет теперь в 6 ГГц. Хорошая новость в том, что разница фактической зоны обслуживания между 6 ГГц и 5 ГГц не так значительна, как между 5 ГГц и 2,4 ГГц.

## Переиспользование Каналов 6 ГГц

Концепция планов переиспользования каналов для 6 ГГц совершенно изумительна. Как показано на Рисунке 13.42, там будет 59 новых 20 МГц каналов, доступных по всем 4 U-NII полосам в Соединенных Штатах. В Европе будет 24 новых 20 МГц канала, доступных в полосе U-NII-5. Одноканальная интерференция не должна быть проблемой с таким большим количеством доступных 20 МГц каналов.

**РИСУНОК 13.42** Каналы 6 ГГц



Однако, так как все частотное пространство доступно в 6 ГГц, ожидается, что использование планов переиспользования 40 МГц каналов станет стандартной практикой. В Соединенных Штатах, 29 новых 40 МГц каналов может быть использовано в плане переиспользования каналов. Еще раз, если все 29 40 МГц каналов используются, одноканальная интерференция (CCI) не должна быть проблемой. В Европе, будет 12 новых 40 МГц каналов, доступных для плана переиспользования. Существует даже предположение, что использование 80 МГц каналов может стать реальностью для копоративных установок 6 ГГц.

В Соединенных Штатах 14 каналов доступно для плана переиспользования 80 МГц каналов.

Вы можете спросить, как на счет уровня шума? Как вы узнали ранее в этой главе, одна проблема с объединением каналов в том, что оно обычно приводит к более высокому уровню шума на 3 дБ. Если уровень шума на 3 дБ выше, то уровень шума (SNR) на 3 дБ ниже, что означает, что радиомодули могут переключаться на более низкие скорости MCS и более низкие модуляции скоростей передачи данных. Во многих случаях, это уменьшает некоторое увеличение ширины полосы, которое предоставляет 40 МГц частотное пространство. Если развернуты 80 МГц каналы, то уровень шума фактически на 6 дБ выше, а SNR на 6 дБ ниже. Разве это не относится к 6 ГГц?

Интригующая разница в 6 ГГц в том, что будут новые правила спектральной плотности мощности [*power spectral density (PSD)*], которые могут уменьшить увеличение в уровне шума, вызванного объединением каналов. PSD - это мера изменения силы сигнала (энергии) как функция от частоты. Единица PSD – это энергия на частоту (ширину), например, 5 дБм/МГц. Для внутренних мало-мощных 6ГГц ТД, FCC определил максимальную ЭИИМ [EIRP] в 36 дБм, на основе спектральной плотности мощности [*power spectral density (PSD)*] в 23 дБм/МГц ЭИИМ [EIRP]. Для внутренних клиентов 6 ГГц, FCC определила максимальный ЭИИМ 30 дБм, на основе PSD 17 дБм/МГц. Более специфично, FCC разрешит максимальную излучаемую плотность спектральной мощности в 5 дБм на 1 мегагерц.

На текущий момент существует много предположений, что правило 5 дБм/МГц компенсирует увеличение на 3дБ уровня шума при объединении каналов. В результате 80 МГц каналы на предприятии могут быть приемлемы. Держите в голове, что 6 ГГц Wi-Fi еще не проверялся в полях, следовательно, остается наблюдать станет ли модель переиспользования 80 МГц каналов распространенной на предприятиях. Но конечно, модель переиспользования 40 МГц каналов является подходящей. Дополнительно, с появлением 6 ГГц, 80 МГц каналы могут быть уверенно использованы для нескольких ТД, расположенных в определенной области, где используются приложения с высокой шириной полосы, такие как дополненная реальность [*augmented reality (AR)*] и виртуальная реальность [*virtual reality (VR)*].

## Обнаружение ТД 6 ГГц

Когда клиенты Wi-Fi 6E войдут на рынок, они будут использовать улучшенные механизмы обнаружения ТД, которые будут требоваться для сертификации Wi-Fi 6E. Так как существует так много каналов в 6 ГГц полосе, клиентское зондирование может занять значительное количество времени. Удивительно, ожидается, что внеполосный процесс обнаружения будет наиболее широко использоваться, даже для клиентов Wi-Fi 6E, уже ассоциированных с 6 ГГц радиомодулем ТД. Большинство чипсетов, используемых в радиомодулях клиентов Wi-Fi 6E, будут также иметь возможности 2,4 ГГц и 5 ГГц, означая, что они могут также подключаться к ТД, используя устаревшие полосы частот. Трех полосные ТД могут информировать клиентов Wi-Fi 6E, активно сканирующих полосы 2,4 ГГц и 5 ГГц о существующих радиомодулях 6 ГГц, которые также расположены в ТД. Следовательно, есть два, определенных *внеполосных* метода обнаружения [*out-of-band discovery methods*]:

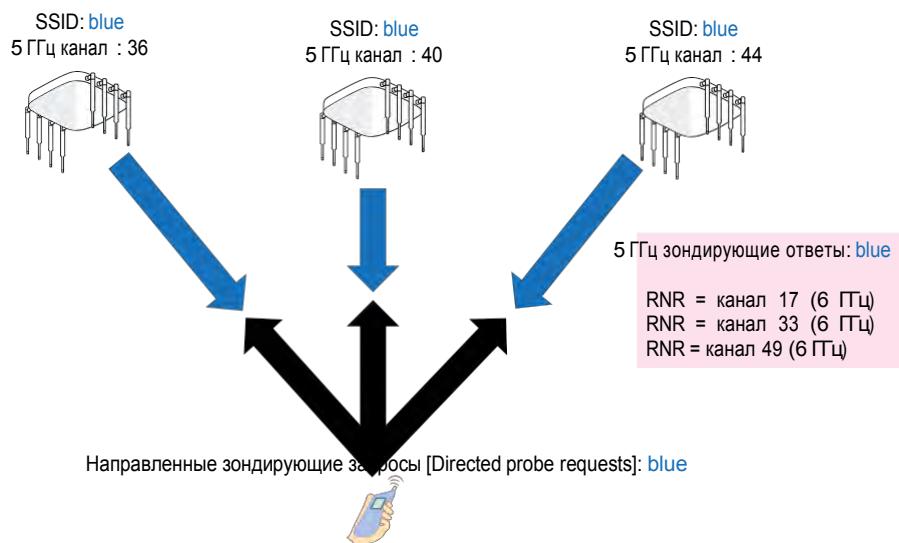
- Уменьшенный отчет о соседях [Reduced neighbor report (RNR)]
- Кадры маяка с несколькими BSSID [Multiple BSSID beacon frames]

802.11v сначала определял возможное использование информационного элемента уменьшенный отчет о соседях [*reduced neighbor report (RNR)*], который может быть использован для включения информации о соседней ТД. Для Wi-Fi 6E, “соседняя ТД” в действительности 6 ГГц радиомодуль, который размещается в той же самой ТД вместе с

радиомодулями 2,4 ГГц и 5 ГГц. Клиенты Wi-Fi 6E узнают о доступном радиомодуле 6 ГГц из информации RNR или из кадров маяка [beacon] или ответе на зондирующий запрос [probe response], отправленных радиомодулями 2,4 ГГц и 5 ГГц ТД.

На примере, показанном на Рисунке 13.43, клиенты Wi-Fi 6E посылают направленные зондирующие запросы [probe requests] по полосе 5 ГГц для SSID с названием *blue*. Три ТД отвечают зондирующими ответами [probe responses], которые несут параметры базового состава сервиса [basic service set (BSS)] для SSID *blue* для 5 ГГц каналов 36, 40 и 44. Однако, внутри каждого ответа на зондирующий запрос [probe response] есть также информация RNR о том же самом SSID, доступном на 6 ГГц каналах 17, 33 и 49. Клиент затем может решить подключаться ли к 5 ГГц, или может даже более вероятно, к доступному 6 ГГц каналу. Очевидно, цель в устраниении времени зондирования [probing time] на 6 ГГц полосе. Клиентское устройство может быть проинформировано о доступном 6 ГГц BSS даже без сканирования 6 ГГц полосы.

**РИСУНОК 13.43** Внеполосное обнаружение – уменьшенный отчетов о соседях



Тот же самый внеполосный метод обнаружения используется, когда клиент Wi-Fi 6E зондирует полосу 2,4 ГГц. Ответы на зондирующий запрос [probe response] от радиомодуля 2,4 ГГц в ТД будут отвечать о доступных каналах 2,4 ГГц, а также в информации RNR о радиомодулях 6 ГГц, которые размещены в той же самой ТД.

Итак, а что если клиент подключится к 6 ГГц ТД на канале 17 и захочет переключиться на другую 6 ГГц ТД? Верить тому или нет, но наиболее вероятно метод клиентского активного сканирования снова будет для клиента Wi-Fi 6E зондировать каналы 2,4 ГГц и 5 ГГц, чтобы получить информацию RNR о возможных 6 ГГц ТД, на которые клиент может переключиться.

Еще один возможный внеполосный метод обнаружения использует кадры маяка с несколькими BSSID. *Маяки со множеством BSSID* [*Multiple BSSID beacons*] – это характеристика, которая изначально была специфицирована в поправке IEEE 802.11v. Она уменьшает избыточную служебную информацию кадров управления путем устранения необходимости в нескольких маяках для нескольких SSID или BSSID.

Например, информация SSID/BSSID для трех SSID сотрудников, гостей и голоса может быть собрана в одном кадре маяка. Хотя эта возможность 802.11v не использовалась в прошлом, клиенты Wi-Fi 6E могут воспользоваться ее преимуществом, чтобы пассивно узнавать о нескольких SSID/BSSID, доступных в нескольких полосах, находящихся в одной ТД.

Хотя ожидается, что внеполосное обнаружение будет предпочтительным методом, также существует три потенциальных метода *внупрополосного обнаружения [in-band discovery]* [6 ГГц ТД]:

- Кадры оповещения обнаружения Быстрой Начальной Установки Канала [Fast Initial Link Setup (FILS) discovery announcement frames]
- Кадры незапрошенного ответа на зондирующий запрос [Unsolicited probe response frames]
- Активное сканирование предпочтаемых каналов [Active scans on preferred channels]

Первые два 6 ГГц внутриполосных метода обнаружения являются пассивными. Кадр оповещения обнаружения FILS является аналогом уплотненного маяка. Подключенные по 6 ГГц клиенты могут слышать кадр FILS от 6 ГГц радиомодуля ТД. Пожалуй, 6 ГГц ТД уже знает, что некоторые 6 ГГц клиенты подключены к другим близлежащим 6 ГГц ТД. В этом сценарии 6 ГГц ТД может послать незапрошенные кадры ответов на зондирующий запрос, чтобы пассивно оповестить клиентов Wi-Fi 6E. Еще раз, цель в том, что клиенты не должны зондировать 59 каналов. Следовательно, ожидается, что наименее используемый метод будет активное сканирование по предпочтаемым каналам. С этим методом, клиент Wi-Fi 6 будет посылать зондирующие запросы по каждому 20 МГц каналу. Эти каналы также выступают в качестве первичных каналов, при объединении в 80 МГц канал.

## Безопасность Wi-Fi в 6 ГГц

Также будет обдумывание безопасности Wi-Fi при развертывании Wi-Fi в полосе частот 6 ГГц. Wi-Fi Альянс будет требовать сертификацию безопасности WPA3 для устройств Wi-Fi 6E, которая будет работать в полосе 6 ГГц. Однако, там не будет обратной совместимости поддержки безопасности WPA2. Более того, поддержка Улучшенного Открытого Шифрования [*Enhance Open Encryption (OWE)*] также будет обязательной. В результате вот несколько ключевых выводов о 6 ГГц:

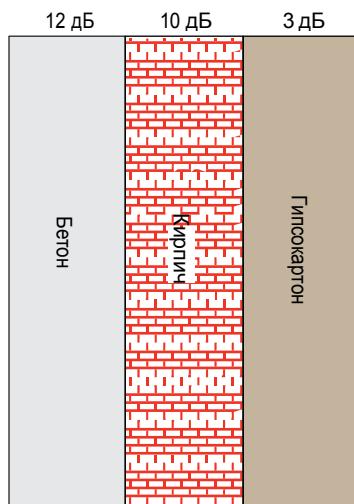
- Так как поддержка OWE будет обязательной, то не будет никакой “открытой” безопасности для SSID, работающей в 6 ГГц. OWE обеспечивает шифрование без аутентификации. Это может иметь некоторые последствия для “гостевых SSID”, которые часто не используют шифрование. Возможно понадобится использовать другой SSID, специально для 6 ГГц. Поддержка безопасности OWE является опциональной для клиентов 802.11ax в 2,4 ГГц и 5 ГГц; однако, OWE на текущий момент редко поддерживается.
- Так как нет обратной совместимости для WPA2, то не будет поддержки для аутентификации PSK. WPA3-Personal, заменяющая PSK, является одновременной аутентификацией равных [*simultaneous authentication of equals (SAE)*]. WPA-3 Enterprise будет продолжать использовать 802.1X. Защита кадров управления [*Management frame protection (MFP)*] также будет требоваться.

Более глубокое обсуждение о безопасности WPA2 и OWE можно найти в Главе 17.

## Физическая Среда

Всегда держите в уме, что физическая среда каждого здания и этажа – различна. В ранние дни Wi-Fi, покрытие было единственной заботой, и чем больше эффективная зона действия, тем лучше. Затухание, вызванное стенами, обычно имело негативное влияние, если зона действия была вашей основной целью. Теперь, когда емкость является такой же заботой, затухание в стенах является действительно желательным. Как показано на Рисунке 13.44, различные материалы вызывают разные уровни затухания, когда сигнал Wi-Fi проходит через стены. Например, гипсокартон ослабляет сигнал где-то на 3 dB, в то время как бетон ослабляет сигнал на 12 dB.

**РИСУНОК 13.44** Затухание в стенах



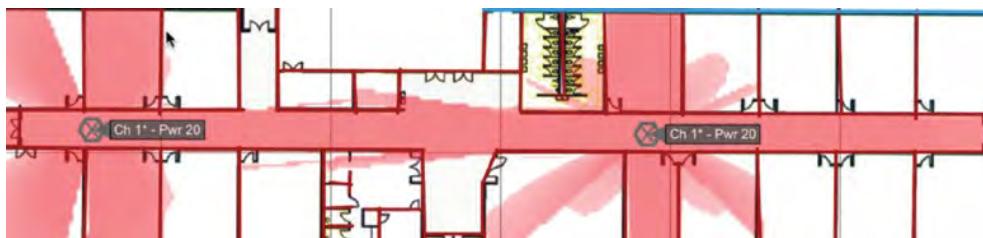
Почему затухание в стенах – это хорошо? В проектах с высокой плотностью, которые теперь широко распространены, с ТД, расположенными в каждом кабинете или через кабинет, затухание в стенах помогает уменьшить одноканальную интерференцию (CCI) и для 2,4 ГГц и 5 ГГц каналов. Вы можете использовать свойства затухания стен, чтобы изолировать домены борьбы за среду, и максимизировать модели переиспользования каналов. Если все внутренние стены гипсокартоновые, то проект с одной ТД на кабинет, обсуждаемый ранее, будет невозможен, даже для 5 ГГц полосы из-за одноканальной интерференции (CCI). Однако, бетонные или шлакоблочные стены ослабят сигнал в три раза или еще больше, чем гипсокартон, что позволяет легче уменьшить CCI.

Место, где вы устанавливаете внутреннюю ТД также очень важно. Большинство ТД имеют внутренние всенаправленные антенны, которые обеспечивают 360 градусов горизонтального покрытия, но только ограниченное количество вертикального покрытия. По этой причине, эти ТД никогда не должны устанавливаться выше 8 метров (25 футов) над землей. Если потолки выше, чем 8 метров (25 футов) (например, в атриуме или складе), наиболее вероятно понадобятся направленные антенны. Всегда проверяйте рекомендации производителя БЛВС по монтажу ТД.

Важный аспект монтажа ТД – “фактор красоты” [“pretty factor.”] Много предприятий предпочитают, чтобы все беспроводное оборудование было полностью скрыто от глаз. Эстетика чрезвычайно важна в розничных магазинах

больницах, и отрасли гостеприимства (рестораны и гостиницы). Однако, заказчики БЛВС часто жертвуют хорошим дизайном БЛВС в пользу эстетики. Например, больницы и гостиницы могут настоять на том, чтобы ТД не монтировались в больничных палатах или гостевых комнатах. Вы когда-нибудь задумывались, почему Wi-Fi во многих гостиницах такой плохой? Wi-Fi часто плох, потому что все ТД установлены по прямой линии по всему коридору отеля, а не внутри комнат. Как показано на Рисунок 13.45, монтаж всех ТД в коридоре является распространенной ошибкой, потому что это вызывает кошмарную одноканальную интерференцию (CCI). ТД и клиенты на одном и том же канале гарантировано будут слышать друг друга несмотря на огромные физические расстояния между устройствами. Монтаж ТД в коридоре обычно не обеспечивает адекватного покрытия в номерах, особенно в отелях с много-комнатными номерами. Всегда монтируйте ТД внутри комнат, где располагается основная масса клиентских устройств, и используйте свойства затухания в стенах в свою пользу.

**РИСУНОК 13.45** Коридоры – это плохо!



## Антенны

Проект БЛВС определяет правильное размещение точек доступа и настроек мощности. Также на плане должно быть указано местоположение распределительных коммутационных щитков, шкафов и стоек. Нужно соблюдать аккуратность, чтобы гарантировать, что размещение точки доступа находится в пределах 100 метров (328 футов) по кабелю от коммутационного узла, из-за ограничений по длине кабеля Ethernet. Убедитесь, что вы учитываете, как вертикальную длину кабеля, так и горизонтальную.

Еще одна, часто не замечаемая, компонента в проекте БЛВС – это использование направленных антенн. Много установок БЛВС используют только заводские с низким усилением всенаправленные антенны, которые обычно имеют усиление где-то от 2 до 5 дБи. Здания бывают разных форм и размеров, и часто у них длинные коридоры, где покрытие внутренних направленных антенн может быть намного более выгодным. Это обычное дело для патч-антенн быть подключенными к точкам доступа для обеспечения направленного покрытия внутри зданий. Так как всенаправленными антennами часто сложно обеспечить адекватное радиопокрытие в местах со стеллажами, то MIMO патч-антенны, такие как представленные на Рисунке 13.46, могут быть эффективно использованы в библиотеках, складах, и розничных магазинах с длинными пролетами стеллажей.

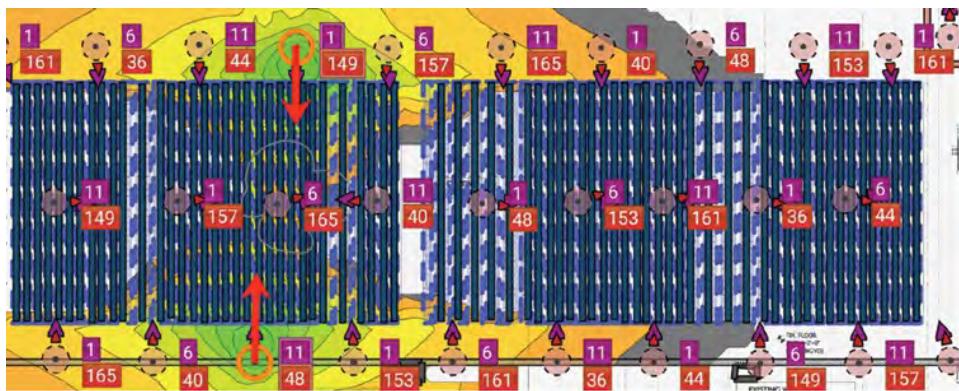
Рисунок 13.47 изображает использование направленных антенн на складе с длинными коридорными линиями из металлических стоек. Патч антенны монтируются на стенах и направляются через проходы и металлические стойки для обеспечения покрытия. Заметьте, что патч-антенны смешены (как шахматная доска) на противоположных

сторонах здания.

**РИСУНОК 13.46** МIMO патч-антенна

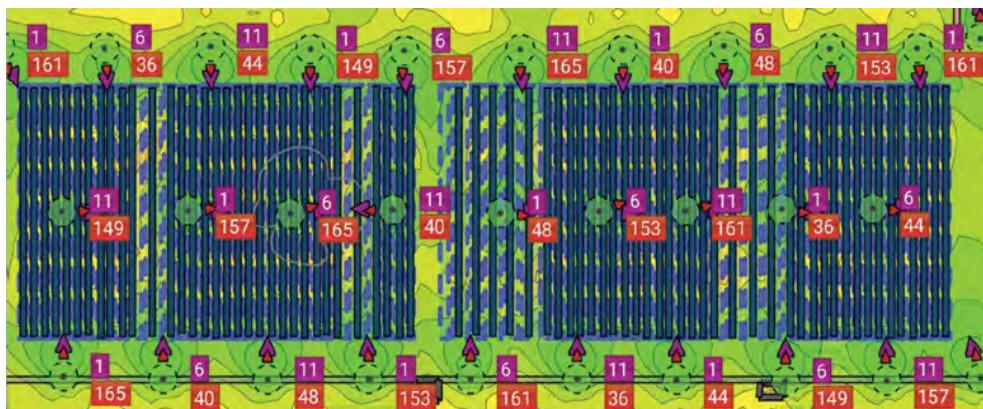


**РИСУНОК 13.47** БЛВС складского помещения — направленные антенны



Покрытие, а не емкость, обычно является первым вопросом в складских средах. Клиентские устройства – это обычно ручные сканеры штрих –кодов или другие беспроводные устройства по сбору данных, которые используются при управлении материально-техническими ресурсами. VoWiFi также является обычным во многих установках БЛВС на складах. Так как большинство складов имеют очень высокие потолки, покрытие, в первую очередь обеспечивается направленными антennами, установленными на стенах и направленных в пролет вниз. Однако, так как многие пролеты являются очень длинными, направленные антенны часто также монтируются на потолок. Как показано на Рисунке 13.48, установленные на потолке направленные антенны, установленные в центре пролета, обеспечивают покрытие совместно с направленными антennами, установленными на стенах.

**РИСУНОК 13.48** БЛВС склада—покрытие стеновым и потолочным монтажом



Еще один распространённый используемый вариант для установки ММО патч-антенн внутри помещений – это среды очень высокой плотности [very high-density (VHD)]. Примером может быть школьный спортивный зал или актовый зал, набитый людьми, использующих несколько радиомодулей Wi-Fi. В сценариях VHD, всенаправленная антenna не является лучшим решением для покрытия, из-за нескольких ТД, установленных на одной и той же открытой территории. ММО патч-антенны часто устанавливаются на стенах или под потолком для обеспечения сжатого “сектора” покрытия. Даже более эффективный метод будет – установка патч-антенн под полом или под сиденьями, или лавочками. ММО патч-антенны направляются вверх, и учитывают свойства поглощения сигнала людьми. Проектирование в аудиториях, спортивных залах, и других средах VHD может быть совершенно сложным. У большинства производителей БЛВС есть специальные рекомендации в руководствах по развертыванию в VHD. Когда бы не использовались направленные антенны, большинство производителей БЛВС рекомендуют использовать статические каналы и настройки мощности.

Профессионалы БЛВС с многолетним опытом обычно используют различные антенны, и направленные, и всенаправленные, в зависимости от здания и требования к БЛВС. Еще один пример другого типа антенн это направленная антenna-распределительный щиток от Вентев [Ventev's directional Junction Box antenna], как показано на Рисунке 13.49. У этой антены ширина луча 75 градусов по горизонтали и 13,49 градусов по вертикали, и она полезна для установки нескольких ТД, обеспечивающих концентрированные зоны покрытия на небольших участках. Использование направленных антенн уменьшает одноканальную интерференцию (CCI), особенно когда развернута модель переиспользования 40 МГц каналов.

**РИСУНОК 13.49** Направленная антenna-распределительный щиток

Любезно предоставлено компанией Вентев [Ventev]



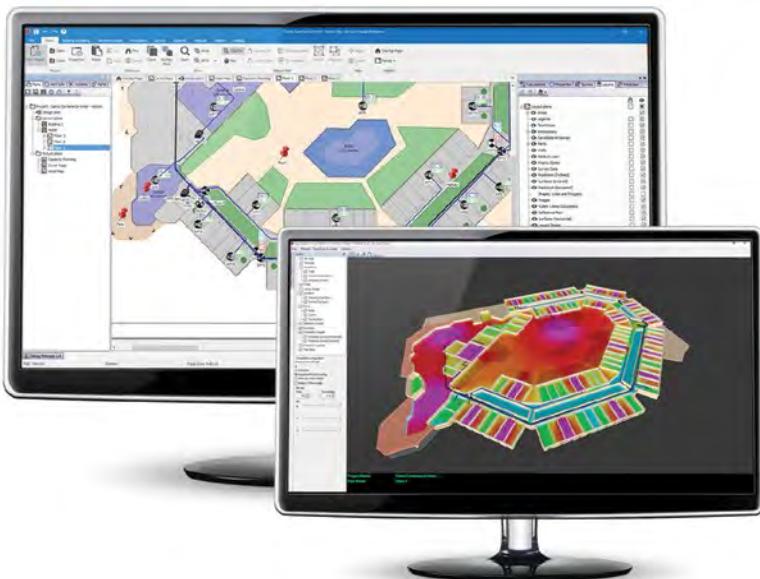
Эта направленна антenna может поворачиваться по одной оси от 0 до 45 градусов, делая ее идеальной для лекционных залов, конференц-центров, больших залов заседаний, и других сред высокой плотности с дизайном непосредственной близости. У антены-распределительного щитка есть 180 сантиметровый (6 футовый) антенный кабельный ввод, который облегчает головную боль при установке, позволяя разместить точку доступа вдали от места установки антены. Физические размеры антены-распределительного щитка Вентев [Ventev Junction Box] достаточно большие так, что некоторые ТД также могут разместится в распределительной коробке вместе с антенными элементами. Что касается эстетики, то закрывающая панель антены-распределительной коробки визуально исчезает в любой схеме внутреннего дизайна. Антена может быть установлена на твердом потолке или на подвесной потолочной плитке. Варианты наклона этой антены позволяют быть установленной параллельно или перпендикулярно полу, и горизонтально или вертикально на стене.

Другие среды БЛВС, которые могут также требовать специальных антенн, включают стадионы и арены. Как упоминалось ранее, проекты ультра высокой плотности требуют профессионалов БЛВС с экспертизой по стадионному Wi-Fi. Несколько производителей БЛВС производят специальные стадионные ТД, которые подразумевают установку под стадионными сиденьями. МИМО патч-антенны также предназначены для установки на мачты и на поручни (или направляющие).

Покрытие сотовым LTE стадионов и арен часто планируется тем же самым интегратором, который создает проект Wi-Fi. Некоторые решения по предиктивному моделированию, такие как iBwave Design, предлагают возможности проектировать обе технологии. Как показано на Рисунке 13.50, основное программное обеспечение по предиктивному моделированию предлагает двухмерный и трехмерный виды радиопокрытия.

**РИСУНОК 13.50** Покрытие стадиона —3D вид

Любезно предоставлено компанией айБвэй [iBwave]



## Наружное Проектирование

Целую отдельную главу можно написать о наружном проектировании Wi-Fi и установке. Наружный Wi-Fi часто используется для покрытия на таких территориях, как парковки, парки, и причалы. Наружное покрытие часто планируется для окружающих здания территорий, которые также предлагают внутреннее покрытие. Пользовательская плотность обычно не является большим вопросом при проектировании наружного покрытия БЛВС. Установка наружного БЛВС часто требует использование взаимосвязанного [mesh] БЛВС, так как Ethernet кабель не может быть легко предоставлен на наружной территории покрытия. Взаимосвязанной [mesh] точке ТД нужно подключиться по транзитному каналу [backhaul link], предоставляемому взаимосвязанным [mesh] порталом, который обычно монтируется на здании с проводным доступом.

Другое типовое использование установок внешнего Wi-Fi – это канал связи типа беспроводной мост точка-точка между зданиями. Мосты БЛВС требуют много вычислений, таких как зона Френеля, потеря на пути в свободном пространстве, бюджет линии связи, и запас на замирание. Большая информация о проблемах и аспектах и внешних взаимосвязанных [mesh] каналов, и мостов БЛВС обсуждается в нескольких главах этой книги. При развертывании наружной взаимосвязанной [mesh] Wi-Fi сети или, пожалуй, внешнего мостового канала связи, администратор БЛВС должен принять во внимание неблагоприятное влияние погодных условий. Следующие погодные условия обязательно должны быть учтены:

**Молния** Прямой и непрямой удар молнии может повредить оборудование БЛВС. Должны использоваться грозоразрядники для защиты от кратковременных токов. Такие решения как молниевывод или медно-оптические трансиверы (медиаконверторы) могут предложить защиту от ударов молнии.

**Ветер** Из-за больших расстояний и узкой ширины луча, узконаправленные антенны чувствительны к движению или сдвигу, вызванного ветром. Даже легкое движение узконаправленной антенны может заставить радиолуч сбиться в сторону от приемной антенны, прервав связь. В очень ветреных средах сетчатая антenna обычно более стабильна, чем параболическая тарелка. Возможно понадобятся другие варианты крепления для стабилизации антенн от движения.

**Вода** Такие условия как вода, снег и туман представляют две уникальные проблемы. Первая, все наружное оборудование должно быть защищено от повреждения, вызванного контактом с водой. Повреждения водой часто являются серьезной проблемой для кабелей и разъемов. Разъемы должны быть защищены капельными петлями и герметизирующей лентой для коаксиальных кабелей для предотвращения просачивания воды и повреждения. Кабели и разъемы нужно проверять на предмет повреждения на регулярной основе. Следует использовать обтекатель (погодозащитная крышка) для защиты антенн от повреждения водой или налипания снега.

Внешние мосты, точки доступа, взаимосвязные [mesh] ТД должны быть защищены от погодных стихий путем использования соответствующих корпусов Национальной Ассоциации Производителей Электрооборудования [National Electrical Manufacturers Association (NEMA)]. Осадки также могут вызывать затухание радиосигнала.

Проливной ливень может ослабить сигнал на 0,05 дБ на километр (0,08 дБ на милю) и в 2,4 ГГц и в 5 ГГц диапазонах частот. На очень длинных каналах связи типа мост обычно рекомендуется закладывать системный операционный запас [system operating margin (SOM)] в 20дБ, чтобы компенсировать затухание от дождя, тумана или снега.

**Ультрафиолет [UV]/Солнце** Ультрафиолетовые лучи и окружающая жара от крыш может повредить кабели со временем, если не используется соответствующий тип кабеля.

## ИТОГО

Эта глава обсуждает покрытие БЛВС, емкость и аспекты плана интеграции с концептуальной точки зрения. Профессионалы БЛВС не всегда согласны с проектом БЛВС и могут иметь свои собственные уникальные подходы. Рекомендации в этой главе основаны на многолетнем опыте многих высококвалифицированных специалистов по проектированию БЛВС. Однако, всегда есть различные стратегии проектирования БЛВС, которые могут быть успешными. Мы обсуждали надлежащее проектирование БЛВС и для подключения с высокими скоростями, и для голосового Wi-Fi. Мы обсуждали значимость принимаемого сигнала в -70 дБм или сильнее, и отношение сигнал-шум [SNR] в 20 дБ или выше. Всегда помните, что проектирование надлежащего покрытия базируется на точке зрения клиента БЛВС. Мы обсудили концепцию динамического переключения скорости передачи данных и много аспектов роумингового дизайна.

Мы также обсудили и интерференцию смежных каналов, и одноканальную интерференцию. Большая часть этой главы обсуждала стратегии проектирования переиспользования каналов в 2,4 и 5 ГГц полосах. Обычно предпочтительнее использовать 20 МГц каналы; однако, проект переиспользования 40 МГц каналов может работать, с рекомендованными оговорками, обсужденными в этой главе. Проектирование покрытия – это только часть уравнения. Также важно соответствующее планирование емкости. Почти у всех БЛВС есть требования высокой плотности пользователей; следовательно, планирование на основе уменьшения потребления эфирного времени является обязательным.

Мы также обсудили каналы DFS 5 ГГц полосы, и как они обычно нужны для выполнения требований по емкости высокой плотности. Двойной 5 ГГц дизайн становится широко распространенным вариантом проектирования БЛВС для емкости, а очень часто требуются направленные антенны для обеспечения секторов покрытия для уменьшения одноканальной интерференции (CCI). Мы также дали вам вводные данные по проектированию в 6 ГГц полосе частот, которые будут доступны для Wi-Fi с начала 2021 года.

Всегда помните, что основная цель БЛВС в обеспечении мобильности и беспроводного доступа к сетевым ресурсам. По этой причине, планирование интеграции также является главным компонентом надлежащего проектирования БЛВС. Аспекты интеграции не обсуждались в этой главе, включая дизайн VLAN, безопасность БЛВС, контроль доступа, подключение клиентов, гостевой доступ, и PoE. Все эти аспекты интеграции обсуждаются в других главах этой книги.

## Темы Экзамена

**Определить динамическое переключение скоростей.** Понимать процесс переключения скоростей передачи данных станции на основе RSSI и SNR. Понимать, что радиомодули ТД также переключают скорости.

**Объяснить различные аспекты роуминга.** Понимать, что клиенты принимают решение о роуминге. Знать, что клиентские RSSI, SNR и другие метрики используются для триггерных порогов роуминга. Понимать важность первичного и вторичного покрытия. Описать проблемы с задержкой, которые могут произойти при роуминге. Понимать почему пересечение границы Зего уровня может вызвать проблемы, и решения, которые существуют.

**Определить разницу между интерференцией смежных каналов и одноканальной интерференцией.** Понимать негативное влияние интерференции смежных каналов (ACI) и одноканальной интерференции (CCI). Объяснить почему модели переиспользования каналов минимизируют проблемы.

**Понимать важность переиспользования каналов.** Объяснить, почему модели переиспользования каналов необходимы для минимизации CCI и устранения ACI. Понимать, что CCI обычно невозможно предотвратить в полосе 2,4 ГГц, и что клиенты являются основной причиной CCI. Определить лучшие практики для переиспользования каналов 5 ГГц.

**Объяснить дизайн с 40 МГц каналами.** Описать базовые правила для использования 40 МГц каналов на предприятиях. Объяснить потенциал негативных последствий объединения каналов и почему 20 МГц дизайн более широко используется.

**Объяснить стратегии по уменьшению потребления эфирного времени.** Объяснить выгоды выключения низких скоростей передачи данных и назначение более высоких базовых скоростей, таких как 12 Мбит/с или 24 Мбит/с.

**Определить выгоды от двойного 5 ГГц дизайна.** Понимать, что 2,4 ГГц это негарантированная полоса частот, и для высокой производительности нужно 5 ГГц подключение. Объяснить как программно-определеные радиомодули могут обеспечить двойное 5 ГГц покрытие и емкость.

**Осознавать потенциал 6 ГГц.** Описать будущие принимаемые во внимание факторы при развертывании трех-полосной технологии Wi-Fi 6. Описать клиентов, покрытие,

**612** Глава 13 • Концепции Проектирования БЛВС  
переиспользование каналов, безопасность и методы обнаружения ТД, используемые для 6 ГГц.

**Объяснить, когда использовать направленные антенны.** Понимать важность использования направленных антенн для сред высокой плотности. Объяснить, как МИМО патч-антенны могут помочь уменьшить домен борьбы за среду путем предоставления секторного покрытия внутри помещений.

# Контрольные Вопросы

1. За какое время все Wi-Fi радиомодули должны уйти с канала динамического выбора канала (DFS), когда обнаружен импульс радара?

  - A. 10 секунд
  - B. 30 секунд
  - C. 60 секунд
  - D. 30 минут
  - E. 60 минут
2. Какой параметр подключения клиента БЛВС может подвергнуться негативному влиянию от клиентской балансировки нагрузки между точками доступа?

  - A. Емкость [Capacity]
  - B. Дальность действия [Range]
  - C. Роуминг [Roaming]
  - D. Пропускная способность [Throughput]
  - E. Безопасность [Security]
3. Что потенциально является проблемой, когда включаете 40 МГц каналы в 5 ГГц полосе?  
(Выберите все, что применимо)

  - A. Интерференция смежных каналов [Adjacent channel interference]
  - B. Одноканальная интерференция [Co-channel interference]
  - C. Более высокое отношение сигнал-шум [Higher SNR]
  - D. Более низкое отношение сигнал-шум [Lower SNR]
  - E. Уменьшение зоны действия [Decreased range]
4. Что является рекомендуемым при использовании 40 МГц каналов в 5 ГГц полосе?  
(Выберите все, что применимо.)

  - A. Включить DFS каналы.
  - B. Уменьшить мощность передачи ТД.
  - C. Подтвердить затухание стен.
  - D. Все вышеперечисленное
5. Сколько клиентских устройств может успешно подключиться и работать с ТД?

  - A. 35
  - B. 50
  - C. 100
  - D. 250
  - E. По разному.

6. Что из перечисленного является вопросами, которые нужно рассмотреть при планировании клиентской емкости БЛВС?
- A. Скольким пользователям и устройствам необходим доступ на текущий момент?
  - B. Скольким пользователям и устройствам понадобится доступ в будущем?
  - C. Где расположены пользователи и устройства?
  - D. Какие возможности MIMO у клиентских устройств?
  - E. Какой тип приложений будет использоваться в БЛВС?
  - F. Все вышеперечисленное
7. Какой предпочтительный метод для конфигурации канала и мощности для корпоративной Wi-Fi ТД? (Выберите все, что подходит.)
- A. Адаптивное радио в стандартной радио среде
  - B. Статические настройки канала и мощности в стандартной радио среде.
  - C. Адаптивное радио в сложной радиосреде, с использованием направленных антенн.
  - D. Статические настройки канала и мощности в сложной радиосреде с использованием направленных антенн.
8. Какая самая большая проблема при включении 5 ГГц динамического выбора канала?
- A. Оповещения о переключении канала
  - B. Ложно положительное срабатывание
  - C. Одноканальная интерференция
  - D. Интерференция смежных каналов
  - E. 60 секундный интервал ожидания
9. Чтобы уменьшить потребление эфирного времени и обеспечить лучшую емкость в полосе 5 ГГц, какие скорости передачи данных рекомендуется выбрать в качестве базовых скоростей? (Выберите все, что применимо.)
- A. 6 Мбит/с
  - B. 9 Мбит/с
  - C. 12 Мбит/с
  - D. 18 Мбит/с
  - E. 24 Мбит/с
10. Как долго ТД должна слушать DFS канал, прежде чем начать передавать?
- A. 10 секунд
  - B. 30 секунд
  - C. 60 секунд
  - D. 30 минут
  - E. 60 минут

- 11.** Какая главная причина одноканальной интерференции?
- A.** Микроволновая интерференция на одном и том же канале в пределах зоны слышимости
  - B.** Точки Доступа на одном и том же канале в пределах зоны слышимости
  - C.** Точки доступа на разных каналах в пределах зоны слышимости
  - D.** Клиенты на одном и том же канале в пределах зоны слышимости
  - E.** Клиенты на разных каналах в пределах зоны слышимости
- 12.** Какой процент перекрытия зон (сот) покрытия необходим для обеспечения бесшовного роуминга?
- A.** 10 процентов
  - B.** 15 процентов
  - C.** 20 процентов
  - D.** 25 процентов
  - E.** Это вопрос с подвохом.
- 13.** Сколько каналов должно быть использовано в 5 ГГц модели переиспользования 20 МГц каналов?
- A.** 3
  - B.** 4
  - C.** 8
  - D.** 12
  - E.** На сколько возможно больше.
- 14.** Что является рекомендованным принимаемым сигналом и отношением сигнал-шум (SNR) для обеспечения клиентской VoWiFi связи?
- A.** -70 дБм и 20 дБ
  - B.** -70 дБм и 25 дБ
  - C.** -70 дБм и 15 дБ
  - D.** -65 дБм и 15 дБ
  - E.** -65 дБм и 25 дБ
- 15.** Какой тип интерференции является результатом того, что точки доступа на одном и том же канале или клиенты на одном и том же канале слышат друг друга несмотря на то, что они являются членами разных базовых составов сервиса?
- A.** Межсимвольная интерференция [Intersymbol interference]
  - B.** Интерференция смежных каналов [Adjacent channel interference]
  - C.** Всеполосная интерференция [All-band interference]
  - D.** Одноканальная интерференция [Co-channel interference]
  - E.** Узкополосная интерференция [Narrowband interference]
- 16.** Какой тип интерференции вызван перекрывающимися зонами покрытия с перекрывающимися частотами?
- A.** Межсимвольная Интерференция [Intersymbol interference]
  - B.** Интерференция смежных каналов [Adjacent channel interference]

- C. Всеполосная интерференция [All-band interference]
  - D. Одноканальная интерференция [Co-channel interference]
  - E. Узкополосная интерференция [Narrowband interference]
17. Сколько каналов должно быть использовано в плане переиспользования каналов для полосы частот 2,4 ГГц?
- A. 3
  - B. 4
  - C. 6
  - D. 11
  - E. 13
18. На основе метрик RSSI, вокруг точки доступа существуют концентрические зоны покрытия с разными скоростями из-за переключения вверх и переключения вниз между скоростями данных клиентской станции. Какое корректное название этого процесса, в соответствии со стандартом IEEE 802.11-2020?
- A. Динамический сдвиг скорости
  - B. Динамическое переключение скорости
  - C. Автоматический выбор скорости
  - D. Адаптивный выбор скорости
  - E. Все вышеперечисленное
19. Дано: Wi-Fi клиенты могут бесшовно переключаться на 2ом уровне, если ТД настроены на один и тот же SSID и на те же самые настройки безопасности. Однако, если клиенты пересекают границы Зего уровня, потребуется решение по роумингу Зего уровня. Какое устройство работает в качестве домашнего агента, если применено решение Мобильного IP в среде корпоративного БЛВС, где не установлен ни один БЛВС контроллер?
- A. Сервер управления беспроводной сетью [Wireless network management server (WNMS)]
  - B. Коммутатор уровня доступа [Access layer switch]
  - C. Коммутатор Зего уровня [Layer 3 switch]
  - D. Точка доступа в исходной подсети [Access point on the original subnet]
  - E. Точка доступа в новой подсети [Access point on the new subnet]
20. Какая телекоммуникационная единица измерения трафика равна одному часу телефонного трафика за один час времени?
- A. Ом
  - B. дБм
  - C. Эрланг
  - D. Час телефонного разговора
  - E. Коэффициент стоячей волны по напряжению

# Глава **14**

A black and white photograph of a lighthouse situated on a rocky coastline. The lighthouse is white with a dark lantern room and is surrounded by several buildings, possibly keeper's houses or storage buildings. The foreground shows large, light-colored, layered rock formations. The ocean waves are visible crashing against the rocks in the background under a cloudy sky.

## Обследование места и Контрольное обследование

---

**В ЭТОЙ ГЛАВЕ ВЫ УЗНАЕТЕ О СЛЕДУЮЩЕМ:**

✓ **Интервью об обследовании места БЛВС и Проекте**

- Брифинг с заказчиком
- Бизнес требования
- Требования по емкости и покрытию
- Существующая беспроводная сеть
- Обновление существующей БЛВС
- Подключение к инфраструктуре
- Ожидания по безопасности
- Гостевой доступ
- Эстетика
- Обследование вне помещений

✓ **Особенности обследований вертикальных рынков**

- Правительство
- Образование
- Медицина
- Розница
- Склады и производства
- Много офисное здание

✓ **Устаревшее обследование ТД на палке**

- Анализ спектра
- Анализ покрытия



✓ Гибридное обследование

- Первичное посещение
- Предиктивный дизайн

✓ Контрольное обследование

- Емкость и пропускная способность
- Роуминг
- Задержка и джиттер
- Соединение
- Эстетика

✓ Инструменты Обследования

- Инструменты обследования внутри помещений
- Инструменты обследования вне помещений

✓ Документы и отчеты

- Бланки и документация заказчика
- Предоставляемые результаты
- Дополнительные отчеты



Когда людей просят дать определение беспроводного обследования места, то для большинства обычный ответ в том, что обследование места нужно для определения радиопокрытия. В ранние дни беспроводных сетей, когда было гораздо меньше беспроводных клиентских станций, подключенных к беспроводной сети, это определение было абсолютно корректно.

Однако, для сегодняшних беспроводных сетей нужно не только обеспечивать покрытие, которого добивались, когда выполнялись первые обследования места, но они также должны обеспечивать более высокую пропускную способность для плотных установок станций. Чтобы достичь эти цели, обследование места должно включать в себя намного больше чем просто определение покрытия, включая обзор потенциальных источников интерференции и надлежащего места размещения, установки и настройки оборудования 802.11 и связанных с ним компонентов.

Существует много способов проведения радиообследований места и контрольных обследований. Очень часто методы субъективны. Как много существует различный мнений в отношении проектирования БЛВС, также часто существуют разные мнения о том, как лучше выполнять обследования. В зависимости от того, кто говорит, определение обследования места БЛВС может быть различным. У профессионалов обследований мест часто свои собственные уникальные технические подходы к выполнению обследования места. Однако, большинство проектировщиков БЛВС используют гибридный метод, который включает предиктивные модели вместе с реальными тестированиями, в то время как другие все еще предпочитают метод ТД-на-палке для проверки и оценки сигнала. Какой бы метод не использовался, нужно понимать, что процесс обследования места полностью связан с проектом БЛВС. Надлежащий проект БЛВС не может быть достигнут, пока не будет проведено исчерпывающее интервью для определения пользовательских требований и ожиданий.

С одним из компонентов, с которым все профессионалы обследований места согласятся – это важность контрольного обследования. Подтверждение покрытия, производительность емкости, и тестирование роуминга являются ключевыми компонентами надлежащего контрольного обследования. В зависимости от цели беспроводной сети, могут быть использованы различные инструменты для помощи в обследовании места.

В этой главе, вы узнаете о компонентах и процессе обследования места [site survey]. Эта глава объясняет интервью с клиентом, необходимую документацию, и доводы, которые может понадобится обсудить, для определенных вертикальных рынков. Много приготовлений должно быть сделано прежде чем проводить обследование места БЛВС. Потребности БЛВС должны быть заранее определены, и должны быть заданы соответствующие вопросы. Эта глава далее продолжит объяснять процедуры и инструменты для выполнения необходимых задач, поясняя и устаревший метод ТД-на-Палке, и, теперь более распространенный, гибридный метод. Наконец, вы узнаете о передаваемых клиенту документации и отчеты.

# Интервью об Обследовании места БЛВС и Проекте

Нужно ли еще обследование места? Ответ на этот вопрос – оглушительное да. Если собственник небольшого розничного магазина цветов хочет беспроводную сеть, то проведение обследования места может быть таким простым, как размещение Wi-Fi маршрутизатора для небольших и домашних офисов [small office, home office (SOHO) Wi-Fi router] в середине магазина, с постепенным установлением мощности передачи на более низкие параметры, и проверкой, что соединение еще существует. Проведение обследования места на средних и крупных предприятиях влечет за собой намного больше физической работы и времени. Перед тем как будет проведено реальное обследование, должно пройти надлежащее *интервью об обследовании места и проекте* [*site survey and design interview*], чтобы и обучить заказчика и правильно определить его потребности.

Проводите ли вы обследование ТД-на-палке или гибридное обследование, обязательно нужно провести начальное интервью с владельцами, чтобы определить задачи, требования и цели БЛВС. У разных вертикальных рынков разные требования, и задачи БЛВС вероятно будут уникальными от заказчика к заказчику.

Процесс интервью может состоять от одной встречи (в случае небольшого заказчика) до многих детальных совещаний (в случае большого или сложного заказчика). Во время этого процесса вам нужно узнать об их существующей сети и среде БЛВС, их требованиях по безопасности, их необходимых приложениях, их текущих и планируемых мобильных устройствах, и их целях, и требованиях. Это одна из наиболее критичных компонент по проектированию сети: работа с клиентом по определению требований к сети. Это критично – идентифицировать и задокументировать эти требования, поскольку это будут ключевыми предоставляемыми пунктами для сети, и того, что вы будете использовать для проверки и подтверждения сети при сдаче сети и во время контрольного обследования.

В дополнение к сбору информации о заказчике и его сети, вам также нужно заставить заказчика предоставить вам электронные масштабируемые поэтажные планы зданий и возможных наружных пространств, где потребуется радиопокрытие. Нужно будет сделать заметки о любом специфичном или уникальном запросе на каждом поэтажном плане, включая эстетику или ограничения по монтажу. Вам также нужно будет запланировать время и доступ (специальная проверка безопасности, разрешения и пропуска, экипировка, или могут понадобится средства индивидуальной защиты) так, чтобы вы могли и выполнить обследование ТД-на-Палке, и собрать радиоданные, которые будут использованы для выполнения гибридного обследования с предиктивным проектированием.

Постановка правильных вопросов во время интервью об обследовании места и проекте не только гарантирует, что соответствующие инструменты будут использоваться во время обследования, но также сделает обследование более продуктивным. Самое важное, конечный результат тщательного интервью и тщательного обследования будет правильно спроектированная БЛВС, которая удовлетворяет всем потребностям предполагаемой мобильности, покрытия и емкости. Следующие разделы охватывают вопросы, которые нужно тщательно обсудить во время интервью по обследованию места.

## Брифинг с Заказчиком

Несмотря на то, что технологии 802.11 существуют с примерно 1997 года, многое непониманий и ошибочной информации о беспроводных сетях все еще существует. Так как многие предприятия и люди знакомы с Ethernet сетями, то преобладает представление “просто воткни и включи”. Если беспроводная сеть планируется для вашей компании или для перспективного клиента, настойчиво рекомендуется, чтобы вы сели с руководством, дали им обзор по беспроводным сетям 802.11, и поговорили с ними о том как и почему проводятся обследования места. Вам не нужно объяснять внутреннюю работу MIMO или CSMA/CA; однако, разговор о преимуществах Wi-Fi, а также ограничений БЛВС – это хорошая идея.

Очень вероятно, что у компании уже есть БЛВС и брифинг с заказчиком будет об обновлении существующей БЛВС. Краткое объяснение преимуществ мобильности будет превосходным стартом для заказчика, который заинтересован в развертывании Wi-Fi в самый первый раз.

Обсуждение возможностей полосы и пропускной способности и ожиданиях от технологии 802.11 также очень важно. Корпоративные пользователи привыкли к 1 Гбит/с полнодуплексному подключению к проводной сети. Из-за хайпа производителей и маркетинга, люди часто верят, что сеть Wi-Fi обеспечит им аналогичные или даже лучше полосу и пропускную способность. Руководство нужно будет обучить, что из-за многих факторов, агрегированная пропускная способность БЛВС – это 50 процентов или меньше от рекламируемой скорости передачи данных. Следует также объяснить, что среда – это общая полу-дуплексная среда, а не полнодуплексная. У среднестатистического заказчика много ошибочных концепций относительно полосы БЛВС по сравнению с действительной пропускной способности.

Еще одно подходящее обсуждение – это почему нужны обследование места и проект БЛВС. Очень краткое объяснение как распространяется и затухает радиосигнал должно помочь руководству лучше понять почему радиообследование места нужно для обеспечения надлежащего покрытия и улучшенной производительности. Обсуждение и сравнение БЛВС 2,4 ГГц и 5 ГГц также может быть необходимым. Если руководство правильно проинформировано по основам Wi-Fi и важности обследования места, то ответы на предстоящие технические вопросы будут в более подходящей форме.

## Бизнес Требования

Первый вопрос, который должен быть задан это “Каково назначение БЛВС?” Если у вас есть полное понимание предполагаемого использования беспроводной сети, то результатом будет лучше спланированная БЛВС. Например, у сети VoWiFi другие требования, чем у тяжело нагруженной сети данных. Если назначение БЛВС только в обеспечении пользователем доступа в Интернет, то рекомендации по безопасности интеграции будут другими. Складская среда с 200 ручными сканерами штрих-кодов очень отличается от офисной среды. У больничной беспроводной сети будут другие бизнес требования, чем у беспроводной сети аэропорта. Вот некоторые из вопросов о бизнес требованиях, который нужно будет задать:

**Какие приложения будут использоваться в БЛВС?** Этот вопрос может подразумевать оба смысла и о емкости, и о качестве сервиса (QoS). Беспроводная сеть для графических дизайнеров, перемещающих огромные файлы по БЛВС, очевидно будет нуждаться в большей полосе, чем беспроводная сеть ни для чего кроме сканеров штрих-кодов. Если требуются чувствительные ко времени приложения, такие как голос или видео, возможно нужно предпринять меры для проекта проводного QoS для

**Кто будет использовать БЛВС?** У разных типов пользователей разные потребности в емкости и производительности. Также может понадобится разделить пользователей по организационным целям. Группы пользователей могут быть разделены по отдельным SSID, VLAN'ам или даже разным частотам. Это также важный вопрос в части безопасности.

**Какой тип устройств будет подключаться к БЛВС?** Является ли большая часть устройств ноутбуками или ручными мобильными устройствами? Каковы возможности MIMO устройств? Будет ли разрешено сотрудникам подключать свои персональные устройства к сети? Есть ли у компании стратегия - *принеси свое устройство* [*bring your own device (BYOD)*], и нужно ли решение *управления мобильными устройствами* [*mobile device management (MDM)*]? Ручные беспроводные сканеры штрих-кодов могут быть также отделены в отдельный VLAN или частоту. VoWiFi телефоны всегда помещают в другой VLAN нежели, чем VLAN передачи данных пользователей с ноутбуками. Какие типы устаревших устройств на текущий момент развернуты? Если инфраструктура БЛВС обновляется, то это может быть хорошим временем и для обновления парка клиентов. Будут ли развернуты беспроводные IoT устройства? Многие IoT Wi-Fi устройства могут передавать только в полосе 2,4 ГГц. Некоторые IoT устройства могут работать в полосе 5 ГГц, но не поддерживать DFS каналы. Возможности устройств могут в итоге определить решения по безопасности, частоте, и общий дизайн БЛВС.

**Есть ли какие-либо ограничения по эстетике или монтажу?** Эстетика чрезвычайно важна во многих средах, включая розничные магазины, гостиницы, и больницы. Ограничения могут быть по тому где может быть физически установлена ТД, и эти ограничения могут не способствовать хорошему дизайну БЛВС. Например, больница может предпочесть, чтобы ТД не устанавливались в гостевых комнатах и палатах пациентов, а вместо этого были смонтированы в коридорах. Как вы узнали из Главы 13 “Концепции проектирования БЛВС”, установка ТД в коридорах не очень хорошая идея во многих случаях. Возможно понадобится найти компромиссы относительно того, где устанавливать ТД.

Мы обсуждаем различные бизнес требования различных вертикальных рынков позже в этой главе. Определение цели БЛВС заранее приведет к более продуктивному обследованию места и является обязательным для успешного окончательного проекта БЛВС.

## Требования по Емкости и Покрытию

После того как цель БЛВС ясно определена, следующий шаг – это начать задавать все необходимые вопросы по планированию и проектированию беспроводной сети. Хотя финальный проект БЛВС является завершенным после проведения обследования места, рекомендуется сделать некоторый предварительный проект, на основе потребностей заказчика по *емкости*[*capacity*] и *покрытию* [*coverage*]. Вам нужно будет сесть с копией плана этажа здания и спросить заказчика, где он хочет, чтобы было радиопокрытие. Ответ почти всегда будет – везде. Если планируется развернуть VoWiFi, то ответ вероятно искренен, так как телефонам VoWiFi нужна мобильность и подключение по всему зданию. Более того, из-за стремительного распространения ручных мобильных устройств, широкое покрытие обычно является необходимостью.

Однако, всеохватывающее покрытие может быть и не нужно. Нужен ли пользователям данных на ноутбуках доступ на территории кладовок? Действительно ли им нужно подключение на внешнем дворе? Нужен ручным сканерам штрих-кодов, которые используются на складской территории, доступ в центральном офисе? Ответы на эти вопросы могут варьироваться в зависимости от более ранних вопросов, которые были заданы относительно цели БЛВС. Если вы определите, что определенная область владения не требует покрытия, вы сэкономите деньги заказчика и собственное время, при проведении физического обследования.

### Рассмотрим Бурный рост беспроводных устройств.

Изначально, Wi-Fi сети в основном использовались для предоставления доступа пользователям ноутбуков, которые привели к безудержному росту мобильных устройств с радиомодулями Wi-Fi, которые на текущий момент ведут к эпохе IoT технологий, подключенной по Wi-Fi.

Радиомодули Wi-Fi везде: в смартфонах, планшетах, сканерах и большинстве других мобильных устройств. Хотя мобильные устройства изначально предназначались для персонального использования, большинство сотрудников теперь используют их и на рабочем месте. Сотрудники ожидают, что они смогут подключиться к корпоративной БЛВС с нескольких персональных мобильных устройств. Из-за бурного роста персональных мобильных устройств, нужна политика «принеси свое собственное устройство» [*bring your own device (BYOD) policy*], чтобы определить, как персональные устройства сотрудника могут получить доступ к корпоративной БЛВС. Решение по управлению мобильными устройствами [*mobile device management (MDM)*] также может быть необходимо для допуска и персональных мобильных устройств, и устройств, принадлежащих компании [*company-issued devices (CIDs)*], к БЛВС. Глава 18, “Принеси Свое Устройство (BYOD) и Гостевой Доступ” обсуждает стратегии BYOD и решения MDM более детально.

Wi-Fi отрасль на переломном моменте роста IoT устройств, которое вероятно замедлится, как уже происходило в прошлом. Компании встраивают радиомодули Wi-Fi, Bluetooth, и Zigbee в любой тип электронного или электрического устройства, такого как системы Климат-контроля [HVAC], холодильники, освещение, и множество сенсоров и устройств мониторинга, которые у них есть или которые они могут придумать. Сбор данных и управление удаленными устройствами продолжает двигать развитие рынка IoT. Хотя у устройств IoT ограниченное взаимодействие с пользователем, они могут обеспечить непрерывный или периодический сбор данных, который может быть использован для аналитики.

В зависимости от планировки и материалов, используемых внутри здания, может понадобится некоторое предварительное планирование относительно типа антенн для использования в определенных местах сооружения. Места с высокой плотностью могут требовать полуунаправленные патч-антенны для секторного покрытия, вместо использования всенаправленных антенн. При проведении обследования, это будет подтверждено или соответственно скорректировано.

Наиболее часто пренебрегаемый аспект до проведения обследования места – это определение необходимой емкости БЛВС. Как вы узнали из Главы 13, вы должны рассматривать не только одно покрытие; вы также должны запланировать клиентскую емкость. Необходимость в проекте БЛВС высокой плотности теперь норма. Для того, чтобы беспроводные конечные пользователи испытывали приемлемую производительность, отношение среднего числа пользователей на точку доступа должно быть установлено. Ответ на вопрос о емкости зависит от переменных, включая ответы на более ранние вопросы о назначении БЛВС. Емкость не будет большим вопросом в складской среде, использующей в основном ручные сканеры штрих-кодов. Однако, если требования к передаче данных по БЛВС от средних до тяжелых, то емкость абсолютно будет вопросом. Ниже перечисление некоторых из многих факторов для рассмотрения при планировании емкости:

- Приложения по передаче данных
- Число пользователей и устройств
- Возможности (характеристики) клиентских устройств
- Пиковое/Наименьшее использование
- Обратная совместимость для устаревших устройств

Тщательное планирование покрытия и емкости во время фазы проектирования БЛВС поможет вам определить места размещения ТД и настройки мощности, типы антенн, и зоны покрытия. Физическое обследование места все-ещё будет проводиться для подтверждения и дальнейшего определения требований по покрытию и емкости.

## Существующая Беспроводная Сеть

Причина, по которой вы проводите обследование места БЛВС может быть в том, что вас позвали в качестве консультанта, чтобы зафиксировать существующую установку.

Профессиональные компании по обследованию часто нанимаются для поиска и устранения проблем в существующих БЛВС, которые часто требуют проведения второго обследования места, или обнаруживается, что первое никогда и не проводилось.

Чем больше компаний и людей становятся образованными в технологиях 802.11, тем процент очевидно будет падать. К сожалению, некоторые необученные интеграторы или заказчики просто ставят точки доступа где-нибудь, где они могут ее смонтировать, и оставляют заводские настройки мощности и канала на каждой ТД. Диагностическое обследование будет проводиться и из-за проблем с производительностью и из-за сложностей с роумингом. Проблемы с производительностью часто вызваны радиоинтерференцией, низким отношением сигнал-шум (SNR), интерференцией смежных зон, или одноканальной интерференцией. Проблемы с роумингом могут также быть связаны с интерференцией или быть вызваны недостаточным адекватным покрытием и/или недостаточным первичной/вторичной зоной покрытия для роуминга. Вот несколько вопросов, которые должны быть заданы перед восстановительным обследованием места:

**Какие текущие проблемы с существующей БЛВС?** Попросите заказчик прояснить проблемы. Связаны ли они с пропускной способностью? Наблюдаются ли частые разъединения? Есть ли какие-либо трудности с роумингом? В какой части здания наиболее часто случаются проблемы? Проблемы происходят с одним устройством БЛВС или с несколькими устройствами? Как часто происходят проблемы, и известны ли шаги, которыми можно было бы повторить проблему?

**Есть ли какие-либо известные источники радиоинтерференции (радиопомех)?** Более чем вероятно, что у заказчика не будет идей, но это не должно останавливать от расспросов. Есть ли какие-нибудь микроволновые печи? Используют ли люди беспроводные телефоны (радиотелефоны) или наушники? Кто-нибудь использует Bluetooth для клавиатуры или мышки? Какие другие беспроводные устройства используются? После выяснение этих интерференционных вопросов, вы всегда должны произвести анализ спектра, который является *единственным* способом, чтобы определить есть ли какая-либо радиоинтерференция на территории, которые могут помешать будущим передачам.

**Есть ли какие-либо известные в покрытии мертвые зоны?** Это связано с роуминговыми вопросами, и области вероятно существуют, где не обеспечивается надлежащее покрытие. Вспомните, это может быть слишком мало или слишком много покрытия. И то и другое создает проблемы с роумингом и со связью.

**Есть ли данные до обследования места и проекта БЛВС?** Возможно, что изначальное обследование места даже не проводилось. Если же старая документация по обследованию места и проект БЛВС существует, то это может быть полезным при поиске и устранении существующих проблем. Важно отметить, что если количественно измеряемые данные не были собраны, которые показывают силу в дБм, то отчет об обследовании следует просматривать с чрезвычайной осторожностью. Кроме того, в сетевой проект могли быть внесены изменения с момента выполнения изначального

**Какое оборудование сейчас установлено?** Спросите какой тип оборудования используется, например: 802.11ac (5ГГц) или 802.11b/g/n (2,4 ГГц), и какого производителя. Рассматривает ли заказчик обновление сети до 802.11ax? Снова, заказчик может не иметь представления, и это будет ваша работа определить, что установлено и почему не работает надлежащим образом. Также проверьте настройку устройств, включая идентификаторы составов сервиса [service set identifiers (SSIDs)], ключи шифрования, каналы, уровни мощности, и версии прошивок. Иногда проблемы могут быть таким простыми, как если все точки доступа работают на одном канале, или есть проблема с буфером, которая решается путем установки последней прошивки.

В зависимости от уровня поиска и устранения проблем, который требуется для существующей беспроводной сети, второе обследование места, состоящее из покрытия и анализа спектра, часто бывает необходимым. После того как проведено новое обследование места, подстройка существующего оборудования БЛВС может быть достаточной. Однако, в худшем случае будет включать полное перепроектирование установки БЛВС. Держите в уме, что когда бы не выполнялось второе обследование места, все те же самые вопросы, которые задаются как часть обследования перед новой установкой (обследование с нуля) [(Greenfield survey)], также должны быть заданы перед вторым обследованием места. Если требования по использованию беспроводной сети изменились, то перепроектирование может быть лучшим направлением действий. Для большей информации о Wi-Fi проблемах и диагностике читайте Главу 15 “Поиск и устранение проблем БЛВС”.

## Обновление Существующего БЛВС

Обновление существующей беспроводной сети является задачей, которую нужно тщательно оценить. Компания может рассматривать установку новых ТД в тех же местах, что и существующие ТД. Это обычно не рекомендуется. Радиопокрытие и форма покрытия новых ТД будут отличаться от радиопокрытия и формы покрытия существующего оборудования. Об этом важно заявить заказчику и заставить его осознать важность проведения нового обследования места и перепроектирования БЛВС.

Разные компании используют разные стратегии при проведении обновления БЛВС. Некоторые компании могут использовать проектный подход “черное и белое” [“salt-and-pepper”], когда сначала обновляются ТД только в определенной области здания. Например, в одной области здания может быть более высокая плотность пользователей и клиентов, поэтому обновление ТД будет сфокусировано сначала на этой области. Другой подход – обновление всего здания на новые ТД, чтобы протестировать новую технологию 802.11 в живой среде предприятия. Если технология надежна, то обновление во всех других здания и местах можно продолжить.

Обычно, циклы обновления БЛВС на предприятиях происходят каждые четыре или пять лет. Как упоминалось несколько раз в этой книге, заказчики БЛВС обычно обновляют свои ТД и БЛВС инфраструктуру, но часто проваливаются с обновлением парка клиентов. Чтобы использовать все преимущества новой технологии 802.11, обновление парка клиентов необходимо. Устаревшие клиенты могут нанести негативное воздействие на общую производительность БЛВС.

## Подключение к Инфраструктуре

Вы уже узнали, что обычные цели БЛВС в обеспечении клиентской мобильности и обеспечении доступа через ТД в существующую проводную сетевую инфраструктуру. Часть процесса интервью включает постановку правильных вопросов так, чтобы БЛВС была правильно интегрирована в существующую проводную архитектуру. Настойчиво рекомендуется спросить копию схем проводной сетевой физической и логической топологии.

По причинам безопасности, заказчик может не захотеть раскрывать проводную топологию, и вам может понадобиться подписать соглашение о неразглашении. Это хорошая идея запросить, чтобы это соглашение было подписано, чтобы защитить вас юридически в качестве интегратора. Убедитесь, что кто-то в вашей организации с правом подписи финализирует это соглашение.

Понимание существующей топологии также будет полезно при планировании сегментации БЛВС и предложений и рекомендаций по безопасности. С или без топологической схемы, следующие темы являются важными, чтобы обеспечить желаемое подключение к инфраструктуре:

**Роуминг** Какой требуется уровень роуминга? Любым устройствам, на которых работают ориентированные на соединение приложения, нужен бесшовный роуминг. Бесшовный роуминг обязателен, если развернуты ручные устройства и/или VoWiFi телефоны. Большинство пользователей смартфонов и планшетов ожидают мобильность. Обеспечение безопасного бесшовного роуминга почти всегда является требованием.

Следует также понимать, что могут быть определенные области, где БЛВС спроектирован, что роуминг имеет самый низкий приоритет, например, в местах с высокой плотностью пользователей. Например, спортивные залы, заполненные 800 людьми, могут иметь ТД на потолке с МИМО патч-антеннами для обеспечения одностороннего секторного покрытия. Здесь проект БЛВС с высокой плотностью имеет приоритет, а не мобильность и роуминг.

Еще одно важное размыщение о роуминге – нужно ли будет пользователям при роуминге пересекать границы Зего уровня. Решение мобильного IP или собственное решение по роумингу Зего уровня будет необходимо, если клиентским станциям нужно переключаться через подсети. Особое рассмотрение должно быть уделено роумингу с VoWiFi устройствами, из-за того, что могут возникнуть проблемы с сетевой задержкой.

**Коммутационные шкафы** Где располагаются точки коммутации кабелей? Будут ли находиться места, предусмотренные для установки ТД, в пределах 100 метров (328 футов) по кабелю от коммутационных точек?

**Антennaя Конструкция** Если требуется наружная сеть или мост точка-точка, то может понадобится построить дополнительную конструкцию для установки антенн. Хорошая идея – это запрос строительных схем крыши здания для определения местонахождения конструкционных балок и существующих проходов(проемов) в крыше. Вам могут также понадобятся разрешения на установку оборудования на крыше или монтаж на здании. В зависимости от веса установки, вам может понадобится консультация с инженер-конструктором по строительству.

**Коммутаторы** Будут ли точки доступа подключены кабелем категории 6 (CAT 6) к неуправляемым коммутаторам или управляемым коммутаторам? Категория 5е (CAT 5e) или выше нужна для 802.3at PoE. Неуправляемый коммутатор поддерживает только один VLAN. Управляемый коммутатор будет нужен, если требуется несколько VLANов. Достаточно ли коммутируемых портов? Каков энергетический бюджет коммутатора? Кто будет отвечать за настройку VLANов? Какие скорости портов поддерживаются? Порты коммутатора обычно поддерживают 1 000 Мбит/с; однако, старые коммутаторы могут иметь только 100 Мбит/с порты. У 100 Мбит/с портов недостаточно полосы для трафика по каналу от сети до ТД. Поддерживают ли коммутаторы коммутируемые порты 2.5 Гбит/с, 5 Гбит/с или даже 10 Гбит/с на перспективу?

**PoE** Как будут запитываться точки доступа? Так как ТД обычно монтируются на потолок, то вероятно будет требоваться чтобы Питание по Ethernet [Power over Ethernet (PoE)] удаленно запитывало точки доступа. У заказчика еще может не быть решения PoE на местах, значит будут нужны дальнейшие инвестиции. Если у заказчика уже установлено решение PoE, нужно определить совместимо ли решение PoE с 802.3af, 802.3at (PoE Plus), или даже 802.3bt. А также, является ли решение конечным оборудованием подачи питания [endpoint] или промежуточным оборудованием подачи питания [midspan]? Если заказчик мигрирует на установку точек доступа 802.11ax, то понадобится больше мощности, и тогда будет необходимо оборудование подачи питания 802.3at или 802.3bt.

Независимо от того, что есть у заказчика, важно убедиться, что оно совместимо с тем, что вы предлагаете установить. Если нужно установить PoE инжекторы, то вам нужно удостоверится, что достаточно электрических розеток. Кто будет ответственен за их установку? Если вы устанавливаете двух частотные 4×4:4 точки доступа, они вероятнее всего будут требовать решение 802.3at PoE Plus или 802.3bt для надлежащей подачи питания всем радиомодулям MIMO.

**Сегментация** Как будут БЛВС и/или пользователи БЛВС отделены(сегментированы) от проводной сети? Будет ли вся беспроводная сеть в отдельной IP подсети связана с уникальными VLANами? Будут ли использоваться VLANы, и нужен ли гостевой VLAN? Будут ли использоваться межсетевые экраны для разделения (сегментации)? Какой тип политик доступа пользователей будет применен к различным группам пользователей или устройств? Или беспроводная сеть будет естественным продолжением проводной сети и следовать тем же кабельным схемам, нумерации VLANов, и проектным схемам, что и проводная инфраструктура? В проекте существующей сети, находятся ли VLANы в ядре сети или они находятся на границе сети? Все эти вопросы также прямо связаны с ожиданиями по безопасности.

**Положение о Наименовании** Есть ли уже у заказчика положение о наименовании кабелей и оборудования сетевой инфраструктуры, и будет ли создано еще одно для БЛВС? У многих ТД уровня предприятия теперь есть возможность анонсирования названия ТД в кадре маяка [beacon frame], что делает проведение обследования места намного проще.

**Управление Пользователями** Должны быть обсуждены вопросы относительно RBAC (контроль доступа на основе ролей), регулирование полосы, и балансировка нагрузки. Есть ли у них существующий RADIUS сервер или нужно будет

его устанавливать? Какого типа используется база данных LDAP? Где будут храниться имена пользователей и пароли? Будут ли имена пользователей и пароли использоваться для аутентификации, или будут использоваться клиентские сертификаты? Будет ли предоставляться гостевой пользовательский доступ?

**Управление Устройствами** Будет ли разрешен сотрудникам доступ в БЛВС со своих персональных устройств? Как будут управляться персональные устройства и устройства компании? Хотят ли они предоставлять разные уровни доступа на основе типа устройства – например, смартфон, планшет, персональный ноутбук или корпоративный ноутбук? Может понадобится стратегия BYOD также, как и решение MDM. Как будут защищаться и управляться устройства IoT?

**Управление Инфраструктурой** Как будут управляться точки доступа удаленной БЛВС? Является ли требованием решение центрального облачного управления? Требуется ли решение по управлению размещать у заказчика [on-premises]? Будут ли устройства управляться по SSH2, SNMP, или HTTP/HTTPS? Есть ли у них стандартные параметры доступа [credentials], которые они хотели бы использовать для доступа к этим интерфейсам управления?

**Про IPv6** Поддерживает ли существующая проводная сеть или требуется ли соединение по IPv6? Будет ли корпоративная инфраструктура БЛВС и клиенты БЛВС поддерживать IPv6? Будет ли IPv6 требованием для сети в дальнейшем?

**Про Многонаправленное вещание [Multicast] и Однонаправленное вещание [Unicast]** Поскольку 802.11 это общая среда, то любая передача влияет на все другие устройства, которые совместно используют один и тот же канал. Кадры много направленного вещания (multicast) являются кадрами, которые посылаются нескольким клиентским устройствам в одно и то же время. Кадры многонаправленного вещания [Multicast] обычно используются для потокового видео. Так как несколько устройств должны быть способными понимать передачу, то мультикастовый трафик посыпается с низкой скоростью передачи данных, чтобы все принимающие клиенты могли понять.

Производители используют разнообразные методы по оптимизации утилизации канала. Один из способов — это преобразование кадров multicast в кадры однонаправленного вещания [unicast] и передача кадров отдельным клиентам на более высоких скоростях передачи данных.

Важно знать требования пользователя к сети, и вам нужно выяснить, нужны ли специальные протоколы или методы связи. Понимание необходимых протоколов вместе с тем как оптимизировать их может иметь огромное значение в том, как хорошо работает сеть.

Всеобъемлющее интервью, которое предоставляет подробные ответы о требованиях к подключению к инфраструктуре приведет к более тщательному обследованию места и хорошо спроектированной беспроводной сети. Семьдесят пять процентов работы для хорошей беспроводной сети заключается в предварительной инженерной работе [pre-engineering]. Она создает план действий [road map] для всех других частей.

## Ожидания по Безопасности

Персонал управления сетью абсолютно точно должен быть проинтервьюирован на предмет ожиданий по безопасности. Все потребности в конфиденциальности данных и шифровании должны быть обсуждены. Все требования AAA (аутентификации, авторизации,

## 630 Глава 14 • Обследование места и Контрольное обследование

учета) должны быть задокументированы. Нужно определить, планирует ли заказчик внедрять беспроводную систему обнаружения или предотвращения проникновения [wireless intrusion detection or prevention system (WIDS или WIPS)] для защиты от неучтенных [rogue] ТД и многих других типов беспроводных атак. Старые устройства могут не поддерживать механизмы быстрого безопасного роуминга, и у этих устройств может не быть опции 802.1X/EAP.

Всеохватывающее интервью касательно ожиданий по безопасности предоставит необходимую информацию, чтобы дать компетентные рекомендации по безопасности после проведения обследования места и перед установкой.

Специфичные для разных отраслей регулирующие акты, такие как Акт о Переносимости и Учета Медицинского Страхования [Health Insurance Portability and Accountability Act (HIPAA)], Акт Закон Грэмма - Лича - Блайли [Gramm-Leach-Bliley], и Индустрия Платежных Карт [Payment Card Industry (PCI)], могут быть приняты во внимание при выдаче рекомендаций по безопасности. Для инсталляций для правительства США может потребоваться строгое следование правилам Федеральным Стандартам Обработки Информации [Federal Information Processing Standards (FIPS)] 140-2, и все решения безопасности возможно должны быть FIPS-совместимы.

\*В России регламентирующие вопросы по защите конфиденциальной информации, закреплены в Федеральном Законе № 149 «Об информации, информационных технологиях и защите информации». При разработке ИТ-инфраструктуры критически важные предприятия должны руководствоваться приказом ФСТЭК №239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации». В нем прописаны основные требования к защите информации на таких предприятиях. Федеральный Закон №187 «О безопасности критической информационной инфраструктуры Российской Федерации» описывает правила защиты ИТ-инфраструктуры на предприятиях, работающих в сферах, критически важных для государства. К таким сферам относится здравоохранение, наука, оборона, связь, транспорт, энергетика, банки и некоторая промышленность.

В Европе необходимо учитывать требования по конфиденциальности Общего Регламента по Защите Данных [General Data Protection Regulation (GDPR)].

Все эти ответы должны также помочь в определении того, существует ли необходимое оборудование и программное обеспечение для выполнения этих функций. Если нет, то это будет ваша работа придумать требования и рекомендации, которые могут быть нужны.

## Гостевой Доступ

Хотя первичной целью корпоративных БЛВС обычно является обеспечение сотрудников беспроводной мобильностью, доступ к БЛВС для гостей компании также может быть важным. В сегодняшнем мире, бизнес заказчики ожидают гостевой доступ в БЛВС. Бесплатный гостевой доступ часто рассматривается как услуга дополнительного вида обслуживания [value-added service]. Из-за широкого принятия Wi-Fi в бизнес средах, большинство компаний предлагают некоторый вид беспроводного гостевого доступа в Интернет. Гости получают доступ к БЛВС через те же самые точки доступа; однако, они обычно подключаются через уникальный гостевой SSID.

Первичной целью гостевого БЛВС является предоставление беспроводного шлюза в Интернет для посетителей компании и/или заказчиков. В основном, гостям не нужен доступ к сетевым ресурсам компании. Следовательно, наиболее важный аспект безопасности гостевого доступа – это защита сетевой инфраструктуры компании от гостей.

Во время интервью нужно обсудить разнообразные типы гостевого доступа к БЛВС и решений по безопасности. Как минимум, должен быть отдельный гостевой SSID, уникальный гостевой VLAN, и политики гостевого межсетевого экрана. Дополнительно, может быть нужен перехватывающий веб портал [captive web portal] в гостевом БЛВС. Шифрованный гостевой доступ также становится более распространенным. Доступно много других опций гостевого доступа БЛВС, включая гостевую само-регистрацию или помочь сотрудникам [employee sponsorship]. Для более детального обсуждения о гостевом Wi-Fi доступе обратитесь к Главе 18.

## Эстетика

Важным аспектом установки беспроводного оборудования является “фактор красоты”[“pretty factor.”] Множество предприятий предпочитают, чтобы все беспроводное оборудование оставалось скрыто от взгляда. Эстетика часто чрезвычайно важна в розничной среде, индустрии гостеприимства (рестораны и гостиницы), музеях, и исторических зданиях. Любое предприятие, которое имеет дело с общественностью, часто требует, чтобы оборудование Wi-Fi было скрыто или, по крайней мере, защищено. Производители БЛВС продолжают создавать более эстетически-выглядящее точки доступа и антенны. Большинство ТД для помещений используют внутренние антенны в целях эстетики. Корпуса для крепления под потолком внутри помещений также могут использоваться для оптимизации внешнего вида и ее надежного монтажа. Большинство блоков корпусов может закрываться, что помогает предотвратить кражу или физического взлома оборудования Wi-Fi.

## Обследование Вне Помещений

Некоторое внимание этой книги и экзамена CWNA уделяется обследованию места на открытом воздухе для установки каналов связи типа мост. Вычисления, необходимые для обследований для внешних мостов - это и зона Френеля, выпуклость Земли, потери на пути в свободном пространстве, бюджет канала связи, и запас на замирания. Однако, обследование места на открытом воздухе в целях предоставления общего беспроводного доступа вне помещений для пользователей становится более обычными. Поскольку популярность беспроводных взаимосвязанных [mesh] сетей продолжает расти, внешний беспроводной доступ становится более широко доступным. Нужны будут наборы обследования места на открытом воздухе, использующие взаимосвязанные [mesh] ТД.

Погодные условия, такие как молния, снег, лёд, жара, и ветер, также должны быть внимательно рассмотрены. Наиболее важный рассматриваемый вопрос - это аппаратура, к которой подключаются антенны. Если оборудование не спроектировано для использования на открытом воздухе, то оно должно быть безусловно защищено от погодных стихий с помощью корпусов стандарта NEMA. (*NEMA* означает National Electrical Manufacturers Association [Национальная Ассоциация Производителей Электрооборудования].) Всепогодные корпуса NEMA доступны с широким диапазоном опций, включая обогрев, охлаждение и PoE интерфейсы.

Безопасность также является большим вопросом при установках на открытом воздухе. Нужно рассмотреть возможность найма профессиональных установщиков. Есть сертифицированное обучение по промышленному альпинизму, работам на высоте, курсы по технике безопасности и оказанию помощи при работе на высоте, курсы по профессиональному стандарту "Антеннщик-мачтовик".



Информация о курсах по охране труда и технике безопасности при работе с радиочастотными устройствами в США можно найти на [www.sitesafe.com](http://www.sitesafe.com). Взбирание на башню/мачту может быть опасной работой. Информация о тренингах о работах на мачтах и безопасности в США можно найти на [www.comtrainusa.com](http://www.comtrainusa.com). \*В России существуют разные организации по обучению по охране труда и технике безопасности при работе на мачтах, башнях, работе на высоте. Также есть обучающие курсы по профессиональному стандарту Антенщик-мачтовик.

Нужно будет рассмотреть все правила регулирования мощности радиоизлучения, определенные регулирующей организацией в вашей стране. Если будут использоваться башни или мачты, вам может понадобится связаться с несколькими правительственные агентствами. У местных и государственных муниципалитетов могут быть строительные регулирующие правила, и почти всегда требуется получать разрешение. В Соединенных Штатах, если башня превышает по высоте 200 футов (61 метр) над уровнем земли [above ground level (AGL)] или находится в непосредственной близости от аэропорта, то требуется связываться и с FCC и с Федеральным Управлением Авиации [Federal Aviation Administration (FAA)]. Если будет устанавливаться опора для антенны на крышу, которая больше 20 футов (6 метров) над самым высоким уровнем крыши, то также нужно проконсультироваться с FCC и FAA. В других странах есть похожие типы высотных ограничений. Свяжитесь с соответствующими регулирующими радиочастотными организациями и авиационными организациями для уточнения подробностей.

## Рассмотрение Вертикальных Рынков

Никогда не будет двух точно похожих обследований места. У каждого предприятия свои собственные потребности, проблемы и доводы при проведении обследования. Некоторые предприятия могут требовать уличное обследование, вместо обследования внутри помещения. *Вертикальный рынок [vertical market]* это определенная отрасль или группа предприятий, которые развиваются и продают похожие продукты или услуги. Подробное обсуждение вертикальных рынков можно найти в Главе 20 “Установка БЛВС и Вертикальные Рынки”. Следующие разделы выделяют характерные темы, которые должны быть проверены при рассмотрении БЛВС для определенных вертикальных рынков.

## **Правительство**

Ключевой вопрос при беспроводных обследованиях мест для правительства - это безопасность. Когда ожидания по безопасности подняты во время процесса интервью, то должно быть тщательное рассмотрение всех аспектов планируемой безопасности. Многие правительственные агентства США, включая военных, требуют, чтобы все беспроводные решения соответствовали FIPS 140-2. Другие правительственные агентства могут требовать, чтобы беспроводная сеть была полностью экранирована или выключена в определенное время дня. Перепроверьте экспортные ограничения перед путешествием в другие страны с определенным оборудованием. Соединенные Штаты запрещают экспорт технологии шифрования AES в некоторые страны. В других странах свои собственные регуляторные правила и таможенные требования.

Вероятнее всего потребуется получать специальные пропуска и разрешения от служб безопасности перед проведением обследования для правительственные организаций. Часто требуется идентификационный бэдж или пропуск. На некоторых правительственных объектах в определенных местах понадобится сопровождение.

## **Образование**

Так же как и на правительственных объектах, для образовательных учреждений обычно нужно получать соответствующее разрешение от охраны. Также необходимо помечать точки доступа в закрываемые корпуса, чтобы предотвратить кражу или повреждение. Из-за высокой концентрации студентов, следует принять во внимание плотность пользователей при планировании емкости и покрытия. 12 летние школы в Соединенных Штатах применяют схему использования планшетов 1:1, где у каждого студента в каждом классе есть доступ к планшету. Из-за этой программы 1:1, не является необычным установка точки доступа в каждый класс, чтобы обеспечить потребность в плотности устройств. Это может быть или может не быть корректным решением. Надлежащее обследование места поможет вам определить лучший сценарий по установке. Больше информации о вертикальном рынке образования можно найти на [www.apple.com/education](http://www.apple.com/education) или [edu.google.com](http://edu.google.com).

В студенческих городках (кампусах) беспроводной доступ в основном требуется в зданиях, и очень часто требуются решения по организации мостов между зданиями в студгородке. Некоторые старые учебные заведения были построены таким образом, чтобы служить укрытием от стихийных бедствий. Это означает, что распространение в этих местах ограничено. Большинство школьных зданий используют плотные материалы для стен, такие как шлакоблоки или кирпич, для поглощения звука между классами. Эти материалы также очень сильно поглощают радиосигналы.

## **Медицина**

Один из самых больших вопросов в медицинской среде - это источники интерференции от огромного массива биомедицинского оборудования, которое присутствует на местах. Многие биомедицинские устройства работают в полосах ISM, но за последние несколько лет, стало больше устройств работать в полосах U-NII. Например, известно, что электрокоагуляторы (электроножи) в операционных создают проблемы в беспроводных сетях. Также существует вопрос с возможной интерференцией между радиомодулем 802.11 и биомедицинским оборудованием.

Нужна будет встреча с департаментом, который управляет и обслуживает все биомедицинское оборудование. В некоторых больницах есть ответственный за

отслеживание перемещения и мониторинг всех радиоустройств в здании. Тщательный анализ спектра при обследовании с использованием спектроанализатора чрезвычайно важен и необходим. Мы рекомендуем, чтобы вы сделали несколько проходов по этим территориям и сравнили их, чтобы обеспечить наибольшую вероятность перехвата всех возможных источников радиоинтерференций. Области с плотной установкой в медицинских учреждениях будут требовать 5 ГГц, потому что вам нужен больший выбор каналов, чтобы предотвратить одноканальную интерференцию. Больницы обычно огромны по масштабу, и физическое обследование сайта может занять недели; предиктивное обследование места может значительно сэкономить время. Длинные коридоры, многоэтажность, двери пожарных выходов, отражающие материалы, бетонные конструкции, освинцованные рентгеновские кабинеты, защитное стекло с сеткой из проволоки являются теми физическими условиями, с которыми вы столкнётесь.

Нужно обсудить все приложения, используемые в медицинской среде, во время интервью и обследования. Многочисленные медицинские приложения есть для ручных устройств на iOS и Android [Андроиде]. Врачи и медсестры используют планшеты и смартфоны для доступа к этим мобильным приложениям. Мобильные устройства также используются для передачи больших файлов, таких как рентгеновские снимки. Медицинские карты используют радиомодули для передачи данных на сестринские посты. Разворачивание VoWiFi телефонов является обычным делом в больницах из-за мобильной связи, которую они обеспечивают для медсестер. Wi-Fi системы определения местоположения реального времени [real-time location systems (RTLSs)], использующие активные 802.11 RFID метки, являются распространенной практикой в больницах для отслеживания материальных ценностей. Из-за присутствия пациентов, часто требуется соответствующие разрешения/пропуска службы безопасности и/или сопровождения. Многие приложения основаны на наличии связи, и сбой в подключении может нанести ущерб для работы этих приложений.

## Розница

В розничной среде часто присутствует много потенциальных источников интерференции в 2,4 ГГц. Демонстрационные модели беспроводных телефонов, радио-нянь, и других устройств ISM диапазона могут вызывать проблемы. Стеллажи и ящики хранения товаров, да и сами товары - все являются потенциальными источниками поглощения(затухания) сигнала. Нужно принять во внимание высокую плотность пользователей. Если возможно, обследование объектов розницы (торговых точек) должно быть сделано в разгар сезона покупок, а не в конце января, когда торговые центры пусты.

Беспроводные приложения, которые используются в розничных магазинах, включают в себя ручные сканеры, для сбора данных и контроля товаров. Розница может требовать решения по аналитике Wi-Fi присутствия для мониторинга и отслеживания перемещения покупателей и их поведение. Устройства точек продаж, такие как кассовые аппараты, также могут иметь Wi-Fi радиомодули.

## Склады и Производства

Некоторые из ранних установок технологии 802.11 на складах были для целей учета товара и сбора данных. БЛВС 2,4 ГГц могут быть все еще развернуты, из-за того что все еще существуют ручные устройства, которые используют устаревшие радиомодули 802.11b/g. Покрытие, не емкость, обычно является главной задачей при проектировании беспроводной сети на складе. Склады заполнены металлическими стеллажами и всевозможными товарами, которые могут отражать или поглощать. Использование направленных антенн на складах может быть требованием. Высокие потолки часто становятся

проблемами с монтажом и проблемами с покрытием. Внутренние перегородки из сетки, которые часто используются для отгораживания и защиты определенных территорий, могут рассеивать и блокировать радиосигнал. Бесшовный роуминг также является обязательным из-за того, что ручные устройства будут мобильными. На вилочном погрузчике, который может быстро перемещаться по складу, часто находятся вычислительные устройства с Wi-Fi радиомодулями. Ручные беспроводные сканеры штрихкодов часто заменяют на смартфоны или планшеты, на которых запускают приложение сканер-штрихкодов.

Производственная среда часто похожа на складскую среду в терминах интерференции и проектирования покрытия. Однако, производственное предприятие представляет уникальные вызовы по обследованию, включая безопасность и наличие профсоюзов работников.

Тяжелые станки и робототехника могут представлять вопросы безопасности для обследователя, и должны быть предприняты специальные меры так, чтобы не устанавливать точки доступа там, где они могут быть повреждены другими машинами. Многие производственные предприятия/заводы также работают с опасной химией и материалами. Может понадобится одеть специальную защитную одежду, и может потребоваться устанавливать прочные точки доступа или короба. На технологичных производственных предприятиях часто присутствуют чистые помещения, и обследователю потребуется одевать чистую спецодежду и следовать процедурам чистого помещения, если им вообще будет разрешено попасть в помещение.

Многие производственные предприятия являются объединением цехов с профсоюзом работников. Может понадобится встреча с представителем заводского союза, чтобы гарантировать, что ни одна политика профсоюза не будет нарушена командой по обследованию места.

## Многоофисные Здания

Пока самая большая проблема при проведении обследования в многоофисном здании это присутствие другого оборудования БЛВС, используемого соседними компаниями. Среды офисных зданий чрезвычайно зашумлены беспроводными сетями 802.11b/g/n, которые работают на 2,4 ГГц. Почти наверняка, большая часть БЛВС других компаний в здании будут выставлены на полную силу сигнала, а некоторое оборудование будет на нестандартных каналах, например 2 или 8, которые скорее всего будут интерфеcировать с вашим оборудованием БЛВС. Также вероятно, что другими компаниями будут использоваться каналы 40 МГц и 80 МГц. Понадобится тщательное планирование каналов и мощности в обоих частотных полосах из-за плохого внедрения Wi-Fi другими компаниями в здании. Может понадобится поговорить с другими компаниями в здании.

## Устаревшее Обследование ТД-на-Палке

Определение обследования места БЛВС изменилось с годами. Многие годы, старый метод *ТД-на-палке [AP-on-a-stick]* был единственным методом, используемым для проведения обследования места. Метод ТД-на-палке представляет собой временную установку ТД и проведение пешего обследования места, чтобы определить соответствующую зону покрытия. Затем, вы перемещаете ТД на следующее место и определяете следующую зону покрытия, повторяя этот процесс по всему зданию. Хотя метод все еще эффективен, он часто занимает очень много времени и является

В следующих разделах мы охватим требования по анализу спектра при обследовании ТД-на-палке также, как и требования к анализу покрытия. Во время процесса анализа покрытия, определяются соответствующие места расположения точек доступа, мощности передачи радиомодулей точек доступа, надлежащее использование антенн.

## Анализ Спектра

Перед проведением обследования по анализу покрытия, обязательно нужно определить местоположение источников потенциальной интерференции. Некоторые компании и консультанты продолжают игнорировать *анализ спектра [spectrum analysis]*, из-за стоимости связанной с покупкой необходимого аппаратного анализатора спектра; однако, с уменьшением цен на анализаторы на основе ПК, анализ спектра все больше становится нормой при обследовании места.

Анализаторы спектра – это оборудование из области радиочастот, которые могут измерять амплитуду и частоту электромагнитного сигнала. Специализированное лучшее в отрасли оборудование анализаторов спектра может стоить десятки тысяч долларов (в долларах США), что делает их запретными по стоимости для большинства предприятий и предпринимателей. Хорошая новость в том, что у некоторых компаний есть решения и на аппаратной основе и на программной основе, которые спроектированы специально для анализа спектра при обследовании места для 802.11, и являются значительно менее дорогими. Чтобы провести надлежащее обследование с анализом спектра 802.11, нужно, чтобы анализатор спектра [*spectrum analyzer*] мог просканировать и полосу ISM 2,4ГГц и полосы U-NII 5 ГГц. Несколько компаний продают решения на программной основе, которые работают с USB адаптерами. Как показано на Рисунке 14.1, МетаГик [MetaGeek ([www.metageek.net](http://www.metageek.net))] предлагает выгодный USB адаптер - анализатор спектра [USB-based spectrum adapter], который способен осуществлять мониторинг спектров 2,4ГГц и 5 ГГц. Рисунок также показывает мониторинговое программное обеспечение компании МетаГик [MetaGeek] Chanalyzer [Ченалайзер, ну или Канализатор].

**РИСУНОК 14.1** USB анализатор спектра 2,4ГГц и 5 ГГц Wi-Spy DBx

Любезно предоставлено компанией МетаГик [MetaGeek]



Как показано на Рисунке 14.2, Ekahau ([www.ekahau.com](http://www.ekahau.com)) [обычно называем - Екахай] продает аппаратное устройство все-в-одном по диагностике и измерению при обследовании Wi-Fi, которое имеет встроенный анализатор спектра и несколько радиомодулей 802.11.

#### РИСУНОК 14.2 Ekahau Sidekick [Екахай Сайдкик]

Любезно предоставлено компанией Екахай [Ekahau]



Так почему же анализ спектра так необходим? Если уровень фонового шума превышает  $-85 \text{ dBm}$  в полосе ISM 2,4 ГГц или полосах U-NII 5 ГГц, производительность беспроводной сети может быть жестко снижена. Зашумленная среда может стать причиной того, что данные в передачах 802.11 станут поврежденными. Примите во внимание следующее:

- Если данные повреждены, то циклическая резервная проверка [cyclic redundancy check (CRC)] не пройдет и принимающий радиомодуль 802.11 не отправит кадр ACK передающему радиомодулю 802.11.
- Если кадр ACK не получен исходным передающим радиомодулем, то однократный [unicast] кадр не подтвержден и должен быть отправлен повторно.
- Если интерферирующее устройство, такое как микроволновая печь, вызывает повторные передачи свыше 10 процентов, то производительность или пропускная способность беспроводной ЛВС значительно страдает.

Большинство приложений по передаче данных в сети Wi-Fi могут работать с повторными передачами на 2ом уровне до 10 процентов без какой-либо заметной деградации по производительности. Однако, чувствительные ко времени приложения, такие как VoIP, требуют, чтобы потери более высокого уровня IP пакетов были не более 1 процента. Следовательно, для сетей с Голосом поверх Wi-Fi [Voice over Wi-Fi (VoWiFi)] нужно ограничить повторные передачи на 2ом уровне до 10 процентов или меньше, чтобы гарантировать своевременную доставку VoIP пакетов.

Интерферирующие устройства могут также удержать радиомодуль 802.11 от передачи. Если радиоволновой источник передает с сильной амплитудой, то радиомодуль 802.11 может обнаружить энергию во время процедуры оценки чистоты канала [clear channel assessment (CCA)] и отложить передачу. Если источник интерференции является

непрерывным сигналов, то радиомодуль 802.11 будет непрерывно откладывать передачу, до тех пор, пока среда не станет чистой. Другими словами, сильный источник радиоинтерференции может действительно удержать клиентские станции и точки доступа 802.11 от передачи вообще.

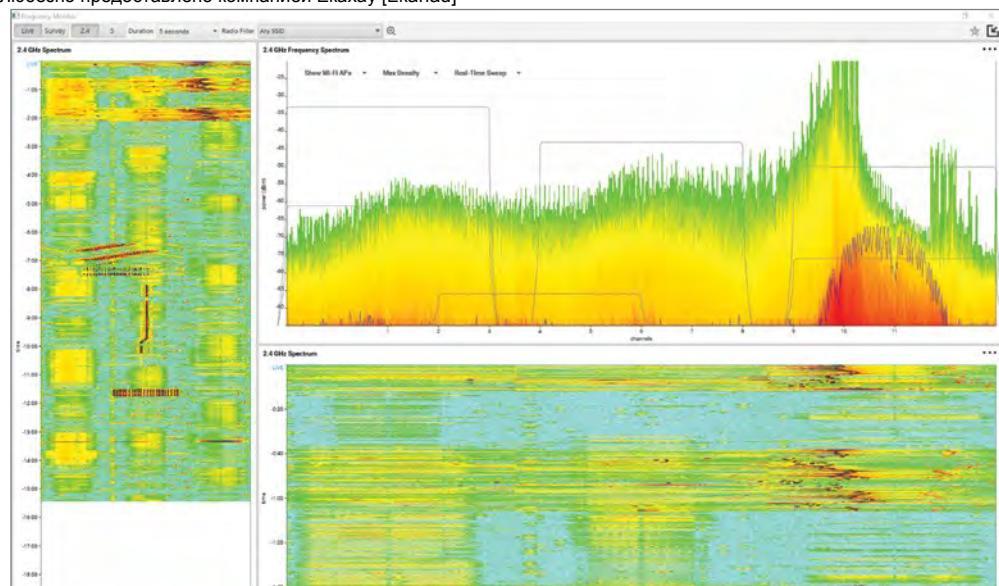
Рекомендуемая практика – проводить анализ спектра во всех частотных диапазонах 802.11. Полоса ISM от 2,4 до 2,5 ГГц – это чрезвычайно переполненное частотное пространство. Вот некоторые потенциальные источники радиоинтерференции в полосе ISM 2,4 ГГц:

- Микроволновые печи
- Беспроводные телефоны в 2,4 ГГц, DSSS, и FHSS
- Люминесцентные лампы
- 2,4 ГГц видеокамеры
- Двигатели лифтов
- Коагуляторы (Прижигающие устройства)
- Аппараты плазменной резки
- Bluetooth радиомодули

Типовые каждодневные источники радиоинтерференции, которые должны быть задокументированы во время интервью по обследованию места – это микроволновые печи. Микроволновые печи обычно работают на 800-1000 ватт. Хотя микроволновые печи экранированы, со временем у них может начать происходить утечка. Микроволновые печи коммерческого уровня экранированы лучше, чем дисконтные микроволновые печи, которые вы можете купить во многих розничных торговых точках. Принимаемый сигнал в -40 дБм – это около 1/10000 милливатта (мВт) и считается сильным сигналом для связи 802.11. Если 1000 ваттная микроволновая печь будет давать настолько малую утечку как 0,0000001 процента, то печь будет интегрировать с радиомодулем 802.11. Рисунок 14.3 показывает вид спектра микроволновой печи. Заметьте, что эта микроволновая печь работает возле канала 11 в полосе ISM 2,4 ГГц. Некоторые микроволновые печи могут фонить по всей полосе частот.

### РИСУНОК 14.3 Вид микроволновой печи на анализаторе спектра

Любезно предоставлено компанией EkaHau [EkaHau]



Вам также нужно проверить использует ли в колл-центр, секретарь, или другие сотрудники мыши, клавиатуры или наушники с Bluetooth. Они также могут вызывать интерференцию.

С появлением 802.11ac, и из-за чрезвычайной переполненности полосы ISM 2,4 ГГц, большинство корпоративных установок переключилось на оборудование 802.11n/ac, которое работает в полосах U-NII 5 ГГц. Переключение на 5 ГГц БЛВС является мудрым выбором для предприятий, потому что 5 ГГц полосы U-NII на текущий момент не очень переполнены, и существует больше выбора для моделей периспользования каналов. Существует не так много интерферирующих устройств. Хотя интерференции в 5 ГГц намного меньше, чем в 2,4 ГГц, это начинает меняться. Также как все перешли с 900 МГц на 2,4 ГГц, чтобы избежать интерференции, эффект перепрыгивания из полосы в полосу [band-jumping] может также коснуться и 5 ГГц.

Также важно отметить, что эволюция технологии Wi-Fi – это уход от спектра 2,4 ГГц. Технология очень высокой пропускной способности [very high throughput (VHT)], определенная поправкой 802.11ac, работает только в полосах U-NII 5 ГГц. Поскольку большинство предприятий разворачивают двухчастотные точки доступа, у которых несколько радиомодулей (фактический устанавливая 2,4 ГГц и 5 ГГц сети одновременно), радиомодуль 2,4 ГГц продолжит поддерживать связь 802.11 b/g/n, в то время как радиомодуль 5 ГГц будет поддерживать связь 802.11a/n/ac. Эти двухчастотные ТД являются важными для обеспечения обратной совместимости со старыми только 2,4 ГГц устройствами. Новые устройства с поддержкой 802.11n/ac/ax выигрывают от подключения к менее загруженным полосам U-NII 5 ГГц, и в то же время поддерживается совместимость для устройств с поддержкой только 2,4 ГГц. На текущий момент потенциальные источники интерференции в полосах U-NII 5 ГГц включают следующее:

- 5 ГГц беспроводные телефоны
- Радары
- Датчики движения (Датчики периметра)
- Цифровые спутники
- Соседние 5 ГГц БЛВС
- Наружные беспроводные мосты в 5 ГГц
- Нелицензируемый LTE

Стандарт 802.11-2020 определяет механизмы *динамического выбора частоты* [*dynamic frequency selection (DFS)*] и *управления мощностью передачи* [*transmit power control (TPC)*] для выполнения регуляторных требований при работе в 5 ГГц полосе, чтобы избежать интерференции с 5 ГГц радарными системами. Как вы узнали из ранних глав, 802.11h-совместимые радиомодули требуются для обнаружения радара на 5 ГГц и выключения передачи во избежание интерференции с радарными системами. Использование анализатора спектра для 5 ГГц во время обследования места может помочь заранее определить есть ли передачи от радаров в этой области, где планируется установка БЛВС. После определения местоположений источников интерференций, самое лучшее и простое решение – это полностью устранить их. Если микроволновые печи вызывают проблемы, рассмотрите возможность покупки более дорогих коммерческого уровня печей, которые менее вероятно, что будут с помехами. Другие устройства, такие как беспроводные телефоны в 2,4 ГГц, должны быть устранены, и должна строго соблюдаться политика, которая их запрещает. Беспроводные телефоны в 5,8 ГГц работают в полосе ISM 5,8 ГГц, которая перекрывается с верхней полосой U-NII (от

5.725 ГГц до 5.850 ГГц). Использование телефонов 5,8 ГГц для помещений будет вызывать интерференцию с радиомодулями 5,8 ГГц, передающими в верхней полосе U-NII.

В прошлом, VoWiFi телефоны работали только в очень загруженной полосе ISM 2,4 ГГц. Сейчас VoWiFi телефоны доступны в 5 ГГц и являются более лучшим выбором для передачи VoIP. Если ваша БЛВС используется или для данных, или для голоса, или для обоих одновременно, то надлежащий и тщательный анализ спектра обязателен для корпоративной среды.

## Анализ Покрытия

После проведения вами спектрального анализа, ваш следующий шаг это крайне важное определение надлежащего радиопокрытия 802.11 внутри вашего здания. Во время интервью об обследовании места и о проекте обсуждаются и определяются требования емкости и покрытия до проведения реального обследования. В конкретной области вашего здания может потребоваться больше ТД из-за высокой плотности пользователей или высоких требований приложений по полосе.

После того как определены все требования по емкости и покрытию, должны быть проведены радиоизмерения, чтобы гарантировать, что эти потребности удовлетворяются и определить соответствующие местоположения и настройки точек доступа и антенн.

**Надлежащий анализ покрытия** [*coverage analysis*] должен быть проведен с использованием измерительного инструмента на основе **силы принимаемого сигнала** [*received signal strength*] или инструмента планирования. Это может быть что-нибудь простое, как измеритель силы принимаемого сигнала в клиентской утилите вашего Wi-Fi радиомодуля, или это может быть более дорогой и сложный пакет программ по обследованию места. Все эти инструменты измерения обсуждаются более подробно позже в этой главе.

Так как вы проведете надлежащий анализ покрытия ? По этому вопросу часто спорят профессионалы индустрии. У многих профессионалов по обследованию есть свои собственные методы; однако, мы попробуем описать базовую процедуру по анализу покрытия с использованием метода ТД-на-палке.

Ошибку, которую многие люди делают во время обследования места – это то, что они оставляют точку доступа с заводскими настройками мощности, установленными на максимум. Хорошая стартовая точка для внутренней точки доступа — это мощность передачи 25мВт. После того, как обследование места проведено, мощность может быть увеличена, если это необходимо, чтобы обеспечить непредвиденные требования по покрытию, или мощность может быть снижена, чтобы удовлетворить потребности по емкости. Большинство ТД двух частотные с 2,4 ГГц и 5 ГГц радиомодулями. Измерения обычно проводятся, используя 5 ГГц радиомодуль, потому что фактическое расстояние зоны действия 5ГГц обычно меньше, чем 2,4 ГГц. Следовательно, использование наименьшего знаменателя 5ГГц диапазона является предпочтительным.



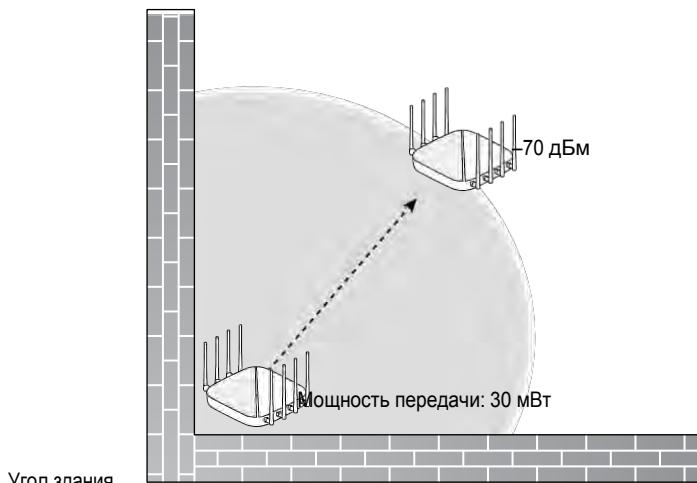
При проектировании покрытия во время обследования места, стандартная рекомендуемая лучшая практика – это обеспечение –70 дБм или более сильный сигнал, который достаточно высок над уровнем шума. Когда вы проектируете БЛВС для клиентов VoWiFi, то рекомендуется сигнал в –65 дБм или более сильный, который еще выше над шумом.

Часто самая тяжелая часть физического проведения обследования места –это найти место, где разместить первую точку доступа и определить границы первой радиозоны (соты). Следующая процедура объясняет, как ее можно определить (и дополнительно

проиллюстрирована на Рисунке 14.4):

1. Поместите точку доступа с мощностью, установленной на 25 мВт (или уровень мощности, который вы определили, как идеальный для вашей среды) в угол здания.
2. Отходите по диагонали от точки доступа в центр здания до тех пор, пока принимаемый сигнал не упадет до  $-70$  дБм, или до той силы сигнала, которую вы запланировали.

**РИСУНОК 14.4** Стартовая зона [cell] покрытия



Во время этого процесса вы должны передавать данные между клиентом и ТД, проверяя не только силу сигнала, но и реальные возможности по передачи. Эта точка и является местом, где вы размещаете вашу первую точку доступа. ( $-70$  дБм будут использоваться в качестве желаемой силы сигнала для пропускной способности далее в этом примере. Если вам нужен другой желаемый уровень сигнала, то используйте его, вместо  $-70$  дБм).

3. Временно установите точку доступа в первом месте, и начните идти по зданию до нахождения конечных точек с  $-70$  дБм, также называемых границами зоны (соты) [cell boundaries] или краями зоны (соты) [cell edges].
4. В зависимости от формы и размера первой зоны покрытия, вы можете захотеть изменить настройки мощности и/или передвинуть исходную точку доступа.

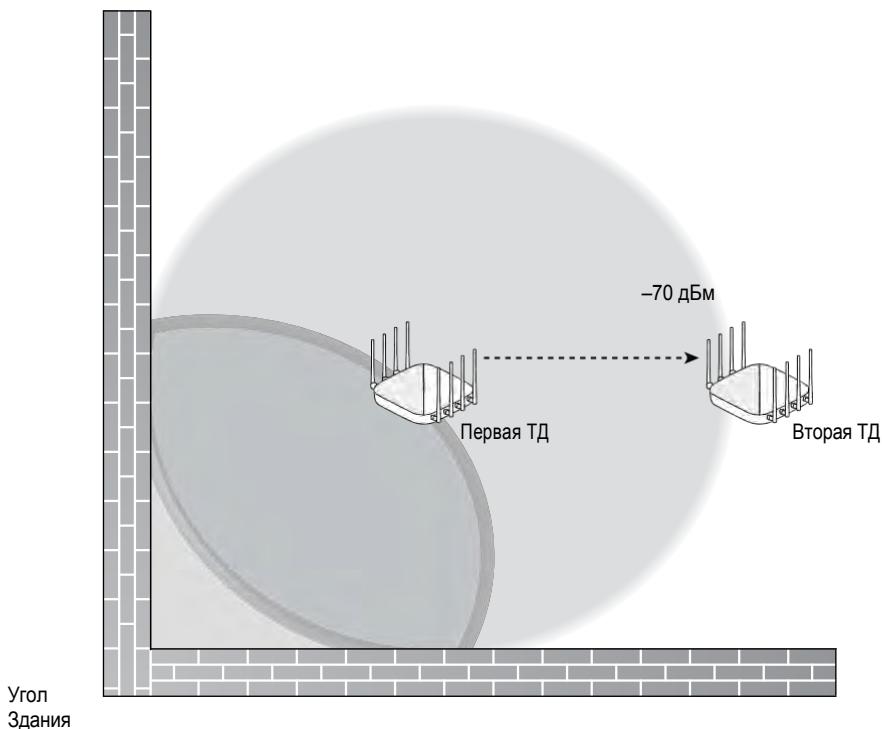
После того, как была определена первая зона покрытия и границы, следующий вопрос – где разместить следующую точку доступа. Местоположение для размещения следующей точки доступа определяется, используя технику, которая аналогична той, что вы использовали для размещения первой точки доступа.

Считайте границу зоны первой точки доступа, где сигнал  $-70$  дБм, как исходную стартовую точку, также как вы использовали угол здания в качестве вашей исходной стартовой точки, и сделайте следующее:

1. От первой точки доступа идите параллельно краю(стене) здания и разместите временную точку доступа в том месте, где принятый сигнал [received signal]  $-70$  дБм, как изображено на Рисунке 14.5.
2. Теперь отходите от этой точки доступа параллельно краю здания до тех пор, пока сигнал не упадет до  $-70$  дБм.

3. Перенесите в это место и временно закрепите точку доступа. ТД, смонтированная в этом месте, обеспечит вторую зону(соту) покрытия.

**РИСУНОК 14.5** Второе положение ТД



4. Начните ходить по зданию, чтобы найти конечные точки с  $-70$  дБм, т.е. границы зоны.  
 5. Снова, в зависимости от формы и размера зоны покрытия, вы можете захотеть изменить настройки мощности и/или переместить точку доступа.

Важно избегать чрезмерного пересечения, потому что это может привести к частому роумингу и деградации производительности. Форма и размер здания и затухание, вызванное различными материалами стен и препятствий, потребует от вас изменить расстояния между точками доступа, чтобы обеспечить надлежащее пересечение зон. После нахождения надлежащего местоположения второй точки доступа и всех ее границ зоны покрытия, повторите процедуру снова. Остальное физическое обследование места, как это, это в основном повторение процедуры снова и снова, фактически по цепочке проходя по зданию, пока не будет определено все необходимое покрытие.

В прошлом, руководства по проектированию БЛВС и информационные материалы от различных производителей БЛВС указывали от 15 до 30 процентное пересечение зон покрытия в целях роуминга. Однако, не существует способа измерить пересечение зон покрытия. Перекрытие зон это в действительности дублированное покрытие с точки зрения клиентской Wi-Fi станции. Надлежащее обследование места должно быть проведено, чтобы гарантировать, что клиент всегда получит надлежащее первичное и вторичное покрытие от нескольких точек доступа. Другими словами, каждой клиентской Wi-Fi станции нужно слышать, по крайней мере, одну точку доступа с определенным индикатором силы принимаемого сигнала [received signal strength indicator (RSSI)] и резервную или вторую точку доступа с таким же RSSI.

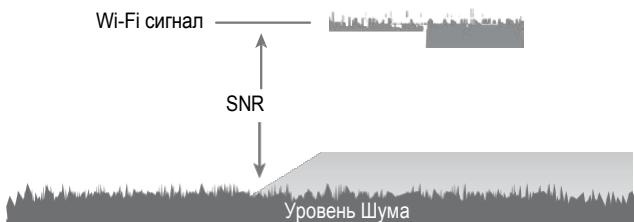
Обычно, пороги RSSI производителей требуют, чтобы принимаемый сигнал был больше, чем  $-70$  дБм для связи с более высокими скоростями передачи данных. Следовательно, клиентским станциям нужно видеть по крайней мере две точки доступа с желаемым уровнем сигнала, чтобы клиент мог при необходимости переключаться (осуществить роуминг).

Во время обследования места проводятся следующие измерения:

- Сила принимаемого сигнала [received signal strength] (дБм), также называется как уровень принимаемого сигнала [received signal level (RSL)]
- Уровень шума [Noise level] (дБм)
- Отношение сигнал-шум [Signal-to-noise ratio, or SNR] (дБ)

Измерения силы принимаемого сигнала, которые записываются во время обследования места, обычно зависят от цели использования БЛВС. Если назначение БЛВС в первую очередь предоставить сервис данных низкой плотности, а не емкость, то можно использовать более низкий сигнал в  $-73$  дБм в качестве границы для перекрывающихся зон. Если пропускная способность и емкость являются более высоким приоритетом, то рекомендуется использовать принимаемый сигнал в  $-70$  дБм или выше. Если вы проектируете БЛВС с клиентами VoWiFi, то рекомендуется  $-65$  дБм или более сильный сигнал, который еще выше над уровнем шума. Отношение сигнал-шум (SNR) является важной величиной, потому что, если фоновый шум слишком близок к принимаемому сигналу, то данные могут быть повреждены и количество повторных передач увеличится. SNR - это просто разница в децибелах между принятым сигналом и фоновым шумом, как показано на Рисунке 14.6. Многие производители рекомендуют минимальный SNR в 20 дБ для сетей передачи данных и минимум 25 дБ для голосовых сетей.

**РИСУНОК 14.6** Отношение Сигнал-Шум (SNR)



*Физический анализ покрытия [Manual coverage analysis]* включает методики, описанные ранее, чтобы найти границы зон. Существует для основных типа ручного обследования по анализу покрытия:

**Пассивный** Во время *пассивного физического обследования* [*passive manual survey*] радиомодуль собирает радиоизмерения, включая силу принимаемого сигнала (дБм), уровень шума (дБм), и отношение сигнал-шум (дБ). Хотя клиентский адаптер на ассоциирован с точкой доступа во время обследования, информация получается от радиосигналов, которые присутствуют на уровне 1 и уровне 2.

**Активный** Во время *активного физического обследования* [*active manual survey*], радиомодуль ассоциирован с точкой доступа и имеет связь на 2ом уровне, позволяя передавать кадры низкого уровня. Если еще установлена связь уровня 3, то трафик низкого уровня, такой как сообщения (пинги или ping) Межсетевого Протокола Контрольных Сообщений [Internet Control Message Protocol (ICMP)], посылаются

в передачах кадров данных 802.11. Радиоизмерения 1 уровня также могут быть записаны во время активного обследования. Однако можно измерить информацию более высоких уровней, такую как потеря пакетов и проценты повторных передач на 2 уровне, так как клиентская карта ассоциирована с одной точкой доступа.

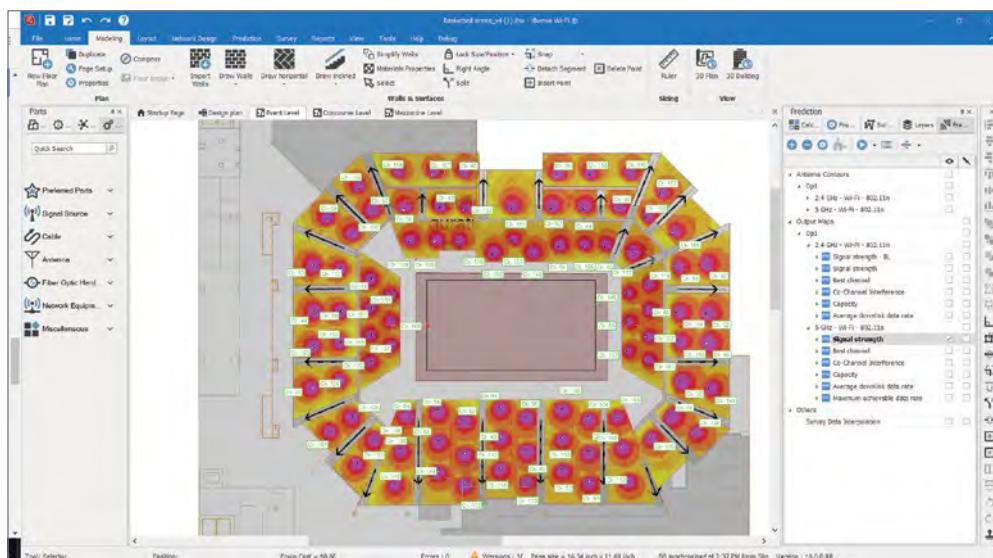
Некоторые производители рекомендуют проводить и пассивное и активное физическое обследование места. Информация от обоих физических обследований затем можно будет сравнить, сопоставить и/или объединить в один итоговый отчет об анализе покрытия. Какие измерительные программные инструменты могут быть использованы для сбора данных, требуемых для пассивного и активного обследований? Существуют многочисленные бесплатные и коммерческие инструменты обследования БЛВС [WLAN discovery tools] для различных операционных систем и устройств.

Некоторые ручные устройства, такие как VoWiFi телефон и Wi-Fi сканер штрихкодов, обладают возможностями по радиообследованию, встроенными в их внутреннее программное обеспечение. Распространенная ошибка, которую совершают обследователи это то, что они держат VoWiFi телефон в горизонтальном положении при измерении радиосигналов во время физического обследования места. Внутренняя антенна VoWiFi телефона обычно имеет вертикальную поляризацию, поэтому удержание телефона в горизонтальном положении может привести к ошибочным измерениям сигнала. Мы советуем держать телефон так, как он обычно используется, а не для того, чтобы создать лучшие данные сигнала.

Коммерческие приложения по радиообследованию, как, например, показанное на Рисунке 14.7, получили широкое признание и в основном обеспечивают лучшие результаты.

#### **РИСУНОК 14.7** Коммерческое программное обеспечение по анализу покрытия при обследовании места

Любезно предоставлено компанией айБвейв [iBwave]



Этот коммерческий пакет позволяет инженеру по обследованию импортировать график плана этажа здания в приложение. Обычно поддерживаются разнообразные графические форматы, и обычно поэтажные планы должны масштабироваться.

Коммерческие приложения работают с клиентскими радиомодулем 802.11 и производят измерения в пассивном физическом(ручном) режиме или в активном физическом(ручном) режиме. Инженер по обследованию ходит по зданию, собирает радиоинформацию и в тоже время записывает местоположение на схеме плана этажа, которое показывает программа. Информация, собранная во время активного и пассивного режимов может затем быть объединена, а визуальное представление радиопокрытия может быть изображено поверх графического плана этажа. Следует отметить, что эти коммерческие приложения по обследованию мест обычно также предлагают двойную функциональность по созданию предиктивных моделей БЛВС, которые будут обсуждаться позже в этой главе.

## Гибридное Обследование

Хотя физический способ обследования ТД-на-палке все еще используется, основная часть профессионалов по проектированию БЛВС и обследованию использует гибридный процесс обследования. Гибридный способ следует многим тем же самым шагам и принципам, что и способ ТД-на-палке, который имеет смысл, поскольку конечная цель также самая: хорошо спроектированная и функциональная БЛВС. В этом разделе вы узнаете о компонентах и шагах, используемых во время гибридного процесса обследования, и вы узнаете сходства и различия между двумя методами.

Основная предпосылка гибридного обследования - это использование радиопредиктивного программного обеспечения для моделирования радиопокрытия в здании или области, где нужен Wi-Fi. Предиктивное программное обеспечение использует мощность радиосигнала ТД вместе с диаграммой направленности антенны, далее использует потери на пути в свободном пространстве и свойства затухания сигнала в стенах; это предсказывает область покрытия каждой ТД в здании. Чем более точную информацию вы вводите в аналитическое программное обеспечение, тем более точная будет предиктивная модель. Следовательно начальное посещение объекта настоятельно рекомендуется.

### Первичное Посещение

После проведения начальных интервью и встреч, вам нужно посетить объект для знакомства с радиосредой, в которой будут работать ТД и клиенты. Перед посещением объекта, убедитесь, что у вас есть несколько копий всех необходимых поэтажных планов и/или цифровыми копиями на ноутбуке или планшете. Цель вашего визита – сделать пометки и задокументировать среду объекта. Данные, которые вы соберете при посещении объекта, будут использованы для создания предиктивной модели.

Вам также нужно убедиться, что у вас есть доступ к зданию и всем комнатам и техническим помещениям. Вам может понадобится сопровождение охраны, или по крайней мере иметь доступ к кому-нибудь с ключами, чтобы предоставить вам необходимый физический доступ. Это может быть невозможным в некоторых местах; однако, важно, чтобы заказчик осознавал, что чем больше доступа и информации у вас будет, тем лучше будет проект.

Еще один вопрос с посещением объекта — это сможете ли вы выполнить его самостоятельно или вам нужен будет второй человек, чтобы помочь вам. Если объект является общественным местом или зданием, вам определенно нужно два человека, поскольку скорее всего будут ситуации, когда вам нужно будет оставить ваше испытательное оборудование, чтобы зайти в другую комнату или на другой этаж, чтобы сделать радиоизмерения. Если заказчик предоставляет вам сопровождение, убедитесь, что они осознают, что посещение объекта включает в себя очень много хождения пешком, и сопровождению нужно быть в подходящей форме, чтобы оставаться с вами во время этого процесса.

## Анализ Спектра

Процесс анализа спектра при гибридном обследовании точно такой же как описано ранее в этой главе в разделе обследование ТД-на-палке. Цель анализа спектра определить любые устройства, вызывающие радиоинтерференцию в полосах Wi-Fi, или которые могут вызвать интерференцию. Информация из анализа спектра будет использована для определения как предотвратить интерференцию при установке БЛВС, или работая вокруг любых интерфеiriющих устройств, или убирая интерфеiriющие устройства. Тщательный анализ спектра нужно сделать по всему зданию.

## Точечные Проверки Затухания

В отличии от обследования ТД-на-палке, которое используется, чтобы определить зоны покрытия при начальном посещении объекта, гибридный метод сначала требует точечные проверки затухания. Перед тем, как выполнять предиктивное проектирование, вам нужно пройти по зданию и сделать заметки и радиоизмерения. Большинство зданий имеют одинаковую конструкцию по всей площади. Стены коридоров, стены ванн, и лестничных площадок обычно сделаны одинаково по всему зданию. Во время обхода по зданию вы будете документировать типы стен вместе с любыми отличиями, если таковые существуют. Вам также нужно делать радиоизмерения объекта, чтобы определить какое затухание вызывается каждым отдельным типом стен. Эта информация будет использоваться в предиктивном проектировании.

Точечные проверки затухания – это фактически периодические измерения ослабления сигнала, которое происходит, когда сигнал проходит через стену. Выполнить измерение просто. Временно установить ТД в комнате в той локации, где ТД может быть установлена по проекту. Настройте на ТД среднюю мощность передачи на 5 ГГц канале с шириной канала 20 МГц. Используйте ручной радиоизмерительный инструмент, или даже ручной смартфон или ноутбук, чтобы измерить принимаемый сигнал от ТД в дБм.

Как показано на Рисунке 14.8, первая оценка сигнала – это измерение *потерь на пути в свободном пространстве* [free space path loss (FSPL)], при этом не должно быть препятствий между вашим измерительным инструментом и ТД. Измерительное устройство должно быть в 15 футах или 5 метрах от ТД, и 1 метре от стены. Для второго измерения, встаньте на продолжении прямой точно с другой стороны стены с измерительным прибором в 3 футах (1 метре) от стены. Разница между этими двумя измерениями и есть затухание, или ослабление сигнала, которое вызвано стеной. Например, первое измерение на Рисунке 14.8 –60 дБм, а второе измерение –72 дБм. Следовательно, затухание стены 12 дБ.

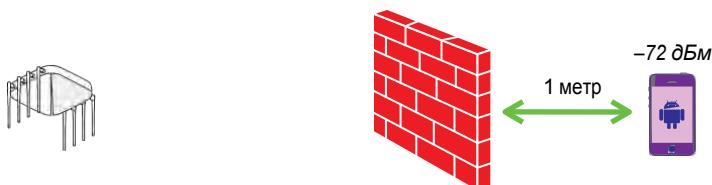
Вы должны делать эти измерения периодически, чтобы гарантировать, что затухание сигнала постоянное по всему зданию для одного и того же типа стен. Если вы подозреваете, что стена построена по другому по сравнению с другими стенами, то вы должны провести измерения и подтвердить величину затухания сигнала. Эти значения должны быть задокументированы и нанесены на ваш план этажа, так чтобы вы могли их использовать позже при создании предиктивного проекта. Точные измерения затухания необходимы для улучшения точности предиктивного проекта.

**РИСУНОК 14.8** Измерение потерь в стене

Первое измерение – потери на пути в свободном пространстве



Второе измерение – с другой стороны стены



## Здание и Инфраструктура

Во время первичного посещения объекта вы должны осмотреть потолки и инфраструктуру на предмет того, сколько усилий понадобится для установки ТД на потолок и протяжку туда кабелей. Кроме того, существует множество других вопросов для обсуждения, которые может понадобится решить. В помещении подвесные ли потолки, гладкие ли отштукатуренные потолки или открытые видимые балки? В дополнение к монтажу ТД, как просто или сложно довести Ethernet кабель до ТД? В большинстве случаев, это также будет значительным вопросом. Должны ли ТД быть скрытыми? Будете ли вы ограничены каким-либо способом в выборе места их монтажа? Есть ли какое-либо другое оборудование, которого вы должны избегать или работать около него? У вас может не быть ответов на эти вопросы, но вам нужно осмотреть и задокументировать любые проблемы и вопросы, которые у вас появились. Обязательно сделайте много фотографий, и убедитесь, что фотографии хорошо задокументированы так, чтобы вы знали что смотреть в дальнейшем. Фотографирование на первоначальном посещении объекта поможет вам во время фазы предиктивного проектирования и во время контрольного обследования.

## Предиктивный Дизайн

Доступно несколько решений по проектированию корпоративного БЛВС и обследованию для создания предиктивного радиодизайна. Следующий список некоторых хорошо известных продуктов, которые могут быть использованы для выполнения такого типа проектирования:

- Ekahau Survey
- iBwave Wi-Fi Suite
- AirMagnet Survey PRO
- TamoGraph Site Survey

Процесс предиктивного проектирования начинается с добавления плана этажа в программу проектирования. В рамках этого процесса важно, чтобы масштаб и размеры плана этажа были точными. Если в здании несколько этажей, план каждого этажа должен также быть надлежащим образом выровнен с этажами выше и ниже. Также обязательно нужно ввести информацию о радиопараметрах, указывая на сколько затухает радиосигнал между этажами.

Чертежи и поэтажные планы часто используют форматы векторной графики ((DWG, DWF) и могут содержать информацию о слоях, включая типы используемых материалов здания. Предиктивное аналитическое программное обеспечение часто поддерживает и векторную и растровую графику (BMP, JPEG, TIF) и позволяет импортировать поэтажные планы здания. Программное обеспечение создает прогнозируемые модели, используя предиктивные алгоритмы и информацию о затухании. Моделируемое прогнозирование может включать следующее:

- Модель переиспользования каналов
- Границы зоны покрытия
- Места размещения точек доступа
- Настройки мощности точек доступа
- Количество точек доступа
- Одноканальную интерференцию [CCI]

После ввода планов этажей, нужно указать все стены, и должны быть указаны параметры радиозатухания для каждой стены. Инженер-проектировщик БЛВС указывает в программе какие используются материалы на плане этажа. В предиктивном приложении уже есть параметры затухания для различных материалов, например для гипсокартона, бетона, и стекла, которые запрограммированы в программу. Также стенам можно указать пользовательские значения затухания. Если план этажа был импортирован в формате схемы *системы автоматизированного проектирования [computer-aided design (CAD)]*, то может быть возможным выбрать все стены определенного типа и универсально назначить значение затухания всем стенам этого типа. Если нет, то вам нужно будет выбрать или определить тип стен, присвоить параметры затухания, и вручную прорисовать стены поверх плана этажа.

После того, как все стены нарисованы и значения радиозатухания им присвоены, вы можете размещать ТД на поэтажных планах. Важно знать марку и модель ТД, которые вы собираетесь использовать, поскольку диаграммы направленности антенн отличаются от одной ТД к другой. Также важно выбрать уровень мощности, который вы планируете использовать для ТД. Настройки ТД и антенны можно будет модифицировать в процессе проектирования, позволяя вам оценивать разные сценарии и варианты.

Как показано на Рисунке 14.9, предиктивное моделирующее программное обеспечение может помочь вам в планировании размещения ТД и желаемом покрытии, и также может визуализировать потенциальную одноканальную интерференцию [*co-channel interference*]. В зависимости от решения, у вас может быть двух мерный или трех мерный вид прогнозируемого покрытия. Все предиктивное программное обеспечение может также автоматически предложить план переиспользования каналов для 2,4 и 5 ГГц полос частот. Большая часть предиктивного программного обеспечения уровня предприятия также предлагает возможность планировать емкость пользователей и устройств. Вы можете обозначить области высокой плотности на плане этажа и ввести число клиентских устройств БЛВС, типы устройств, и использование прогнозируемых приложений.

**РИСУНОК 14.9** Предиктивная модель

Любезно предоставлено компанией Ekahau [Ekahau]



После ввода всех ваших данных и манипуляций, у вас будет в итоге предполагаемый проект, который, как вы полагаете, выполнит ваши требования по покрытию и емкости. Программное обеспечение по проектированию будет способно создать список ТД и антенн (если вы планируете какие-либо внешние антенны). Предполагаемый дизайн со списком материалов [bill of materials (BoM)], может быть использован для помощи при заказе оборудования и установке оборудования.

## Контрольное обследование

Одна часть процесса проектирования и обследования БЛВС, которую часто пропускают — это финальное *контрольное обследование* [*validation survey*]. После того, как беспроводная сеть установлена, и до того, как будет переведена в эксплуатацию, важно провести аудит или проверку установки. Эта проверка позволит вам подтвердить, что радиопокрытие и другие задачи проекта БЛВС выполнены или перевыполнены. В процессе контрольного обследования вы можете сравнить реальные значения с ожидаемыми значениями ваших планов сетевого проекта — проекта ли сделанного с использованием метода ТД-на-палке или с помощью предиктивной модели. Надеемся, что эти значения соответствуют или превосходят ваши ожидания. Если это не так, вам нужно проанализировать почему, и затем определить приемлемо ли реальное покрытие, роуминг и производительность, или вам нужно будет модифицировать вашу установку. Если вы нанимали компанию по проектированию и установке вашей сети за вас, то это подтверждение (валидация) БЛВС является важной, чтобы гарантировать, что они предоставили то, что обещали и что ожидалось.

К сожалению, беспроводная сеть не всегда ведет себя как ожидается. Со временем, или даже внезапно, производительность сети может деградировать. Эта деградация может быть вызвана изменением в том как используется сеть, проблемами с оборудованием или программным обеспечением, неисправностями точек доступа или контроллера БЛВС, или изменениях в окружающей среде, где работает сеть. Любое или все из этого может повлиять на радиопокрытие. В этой ситуации контрольное обследование беспроводной сети должно быть способным помочь вам в определении причины вашей проблемы.

Контрольное обследование беспроводной сети обычно проводится систематическим обходом по зданию или зоне покрытия беспроводной сети, и осуществлением радио и сетевых измерений. Эти измерения затем документируются на плане этажа или карте. Эта информация должна помочь вам определить, где и почему присутствует проблема.

На рынке есть много продуктов, которые могут помочь вам провести контрольное обследование беспроводной сети. Многие те же самые инструменты моделирования обследования могут также быть использованы для проведения контрольного обследования беспроводной сети. Программное обеспечение обследования места позволит вам сделать сетевые измерения, предоставит вам визуальную тепловую карту вашей радиосреды. Это часто включает в себя огромный и утомительный процесс обхода здания с ноутбуком. Вместо того, чтобы ходить с ноутбуком, или в качестве дополнительного ресурса, вы можете использовать профессиональный ручной инструмент контрольного обследования, например показанный на Рисунке 14.10.

**РИСУНОК 14.10** netAlly AirCheck G2

Любезно предоставлено компанией нетАлли [netAlly]



Ручные устройства контрольного обследования обычно обладают повышенной прочностью, чтобы защитить от несчастных случаев и неаккуратного обращения. Инструменты контрольной проверки могут идентифицировать и точки доступа, и клиентские устройства. Они могут предоставить расширенную информацию о точках доступа, SSID, радиосигналах, безопасности, и сетевом трафике вместе с многой другой информацией. Хороший ручной инструмент может обеспечить вас огромным массивом информации и позволит вам понять, что видит клиентское устройство в сети, в надежде помочь вам понять работает ли сеть корректно и, если нет, то почему.

Из-за различия RSSI чувствительности между устройствами БЛВС, контрольное обследование часто выполняется с использованием различных типов клиентов БЛВС. Например, контрольные радиоизмерения могут быть зафиксированы с использованием и профессионального ручного инструмента обследования и менее дорогого смартфона с радиоизмерительным программным обеспечением.

Во время фазы проектирования вы должны задокументировать все области, которые требуют Wi-Fi покрытие. Дополнительно, вы должны задокументировать минимальный уровень покрытия, которое было необходимо—особенно, требуемые dBm уровня принимаемого сигнала и SNR. В большинстве случаев будет требоваться принимаемый сигнал, по крайней мере, -70 dBm и 20dB или больше SNR. Контрольное обследование требует, чтобы вы ходили по объекту и проверяли, что эти требования к радиосигналу удовлетворяются.

Держите в уме, что контрольное обследование - это не просто подтверждение места размещения ТД и покрытия. Вам также нужно подтвердить емкость, роуминг и другие метрики производительности. Контрольное обследование должно также считаться высшим приоритетом, потому что оно дает вам возможность подтвердить, что БЛВС работает надлежащим образом и удовлетворяет всем исходным требованиям к проекту БЛВС. Контрольное обследование требует заинтересованности и трудовых затрат; однако, конечный результат - это счастливые пользователи Wi-Fi. Интересное замечание: несколько производителей на текущий момент работают над прототипом робота по контролльному радиообследованию, которые однажды могут помочь и автоматизировать большую часть процесса радиопроверки.

## Емкость и Пропускная способность

Исследование емкости БЛВС выполнено раньше на фазе проектирования сети. Емкость - это обеспечение достаточного числа ТД для количества клиентских устройств, распределении большого числа устройств по множеству ТД. Во время контрольного обследования вам нужно убедиться, что установленные ТД будут удовлетворять потребностям заказчика. Следовательно, вам также нужно убедиться, что проект сети проверен на соответствие клиентской емкости и требованиям.

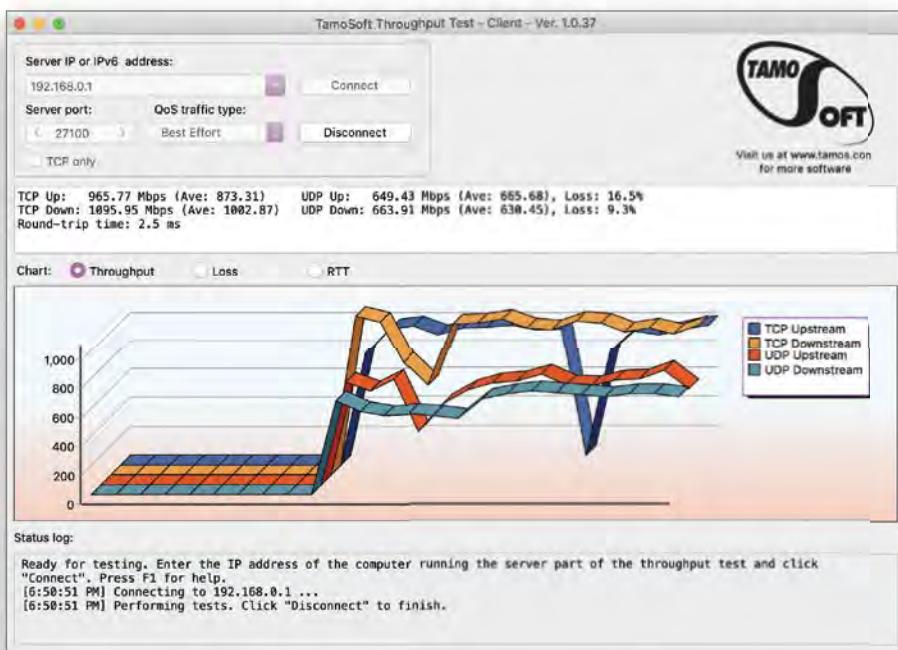
Проверка пропускной способности важна не только, чтобы убедится, что у вас есть сигнал, но и что сигнал достаточно силен, чтобы обеспечить определенный уровень пропускной способности. В дополнение к проверке, что определенные скорости данных 802.11 достижимы, вы должны подтвердить, что проводная инфраструктура работает в соответствии с проектом, и способна обработать то количество данных, которое пройдет к и от ТД и беспроводных клиентов.

Инструменты проверки пропускной способности используются, чтобы оценить ширину полосы и производительности пропускной способности сети. Тестеры пропускной способности обычно работают по клиент/серверной модели, чтобы измерить потоки данных между двумя точками в обоих направлениях. При проверке нисходящей

пропускной способности БЛВС, клиент 802.11 должен быть настроен как сервер. При проверке восходящей пропускной способности БЛВС, клиент 802.11 должен быть настроен как клиент, связывающийся с сервером позади ТД.

iPerf это утилита с открытым исходным кодом, которая обычно используется для генерации TCP или UDP потоков данных, чтобы проверить пропускную способность. Многие производители БЛВС предлагают iPerf в качестве утилиты типа командной строки (CLI) из OS точек доступа. Как показано на Рисунке 14.11, TamoSoft ([www.tamos.com](http://www.tamos.com)) предлагает бесплатное ПО с графическим интерфейсом (GUI), которое доступно для Windows, macOS, iOS, и Android клиентов. Установка включает и клиентское и серверное ПО. Серверное ПО должно работать на проводной сети, а клиентское ПО должно работать на клиенте БЛВС. Клиент и сервер посылают данные друг другу, отображая метрики загрузки в обоих направлениях.

**РИСУНОК 14.11** Тестер пропускной способности TamoSoft



## Роуминг

Если только вы не устанавливаете сеть из одной ТД, то бесшовный роуминг будет требованием для БЛВС. В зависимости от дизайна сети, может потребоваться решение по роумингу 3 его уровня - Мобильный IP, позволяющее бесшовно переключаться между сетями 3его уровня, сохраняя при этом IP адрес. Хотя, технически, это не является компонентом радиопроекта, это потенциально является частью сетевого проекта, и тем, что может потребоваться проверить и подтвердить. Еще один

аспект роуминга, который может понадобиться проверить и подтвердить - это клиентский роуминг при использовании аутентифицированного и зашифрованного 802.1X/EAP клиентского соединения. Это как правило включает проверку механизмов быстрого безопасного роуминга. Ручные проверочные инструменты, упомянутые ранее, часто имеют встроенные возможности по тестированию роуминга. Производительность роуминга также может быть оценена с использованием платформы управления ТД.

## Задержка и Джиттер

Сетевая задержка [*latency*] - это время по доставке пакета от устройства к конечному назначению. Для многих приложений, таких как просмотр веб-страниц и электронная почта, задержка является несущественным, обычно незаметным явлением. Для приложений, таких как VoIP или потоковое видео, однако, любая повторная пересылка пакетов или задержка могут быть очень заметными и раздражающими. В зависимости от сетевого дизайна и требований, вам может понадобиться проверить и подтвердить, что инфраструктура может поддерживать необходимые требования по доставке.

Джиттер [*Jitter*] - это вариация задержки. Джиттер измеряет насколько задержка каждого пакета отличается от средней. Если все пакеты передаются с одной и той же скоростью по сети, то джиттер равен 0. Если в БЛВС высокий уровень повторных передач на 2ом уровне, то джиттер - это обычный результат, приводящий к прерывистому звуку или видео. Большинство приложений БЛВС могут быть терпимы вплоть до 10 процентов повторных передач без какой-либо заметной деградации в производительности. Однако, чувствительным ко времени приложениям, таким как VoIP, нужны намного меньшие уровни, обычно менее 5 процентов, а лучше ближе к 2 процентам. Хороший сетевой дизайн от одного конца до другого конца [end-to-end] должен помочь достичь этих цифр, однако, нужно проверить, чтобы подтвердить, что они достигаются.

## Связь

Еще одна критическая часть БЛВС – это соединение с ядром корпоративной сети, и подключение клиентских устройств БЛВС к корпоративной сети. Проводной инфраструктуре нужно быть способной обработать нагрузку, подаваемую в неё от БЛВС. Инфраструктуре также необходимо быть способной поддержать любую необходимую сегментацию, маршрутизацию, и требования к PoE вместе с любыми другими требуемыми скрытыми функциями. Любые характеристики, поддержку которых вы запрашиваете от инфраструктуры, должны быть проверены и подтверждены.

## Эстетика

Является ли в действительности это частью контрольного обследования или частью всего процесса установки, эстетика является важной частью успешной установки БЛВС. Некоторые среды, такие как исторические здания, могут требовать, чтобы ТД и антенны не были видны. Вы можете выполнить это, устанавливая устройства над потолком, за стенами, или под полом. Вы также можете закамуфлировать ТД, чтобы они выглядели, как и другие части здания, например, встраивая их в лепные украшения или освещение. Какой бы метод установки не использовался, убедитесь, что все выглядят чисто и профессионально. Надлежащий монтаж нужно наблюдать и корректировать во время процесса установки; однако, уделите внимание этому также и во время контрольного обследования, чтобы гарантировать, что ничего не было упущено.

# Инструменты Обследования

Любой, кто серьезно относится к развертыванию беспроводных сетей, собирает вместе набор инструментов для обследования с множеством продуктов, которые могут помочь в процессе обследования места. Главный инструмент будет своего рода устройство измерения сигналов или программная утилита, которая взаимодействует с вашей беспроводной клиентской картой, и используется для анализа сигнала. Предварительно собранные наборы для обследования места можно найти в продаже в Интернете, но многие профессионалы обследования предпочитают собирать свой собственный набор. Обследования мест внутри и снаружи помещений очень различаются. Следующие разделы обсуждают различные инструменты, которые используются в обоих типах обследований.

## Инструменты Обследования Внутри Помещений

Как говорилось ранее, вам нужен будет анализатор спектра, чтобы определить положение потенциальных источников интерференции. Ваше основное оружие в арсенале анализа покрытия будет инструмент измерения силы принимаемого сигнала. Если вы проводите простое обследование места, таким инструментом может быть что-то базовое, как например измеритель силы принимаемого сигнала в утилите(ПО) вашей беспроводной клиентской карты. Для большинства обследований, однако, рекомендуется, чтобы вы использовали более дорогой и сложный пакет программного обеспечения по обследованию. Тем не менее, существует много других инструментов, которые могут помочь вам, когда вы проводите физическое обследование места. Вот некоторые из инструментов, которые вы можете использовать для обследования места внутри помещений:

**Анализатор Спектра**      Этот анализатор нужен для анализа частотного спектра.

**Чертежи**      Чертежи или планы этажей здания нужны, чтобы нанести карту покрытия и указать параметры радиоизмерений. Программное обеспечение САПР [CAD] может понадобиться для просмотра и редактирования цифровых копий чертежей.

**Программное Обеспечение по Измерению Силы Сигнала**      Вам нужно это ПО для анализа радиопокрытия.

**Клиент БЛВС или Ручной Контролирующий Инструмент**      Вам будет нужен подключенный к БЛВС ноутбук, планшет или смартфон с программой по измерению сигнала. Опционально, вы можете использовать более дорогой ручной инструмент контрольного обследования.

**Точка Доступа**      По крайней мере, одна ТД будет нужна, желательно больше. Точки доступа могут быть использованы как отдельно стоящие устройства во время обследования или первичного посещения объекта. Управляемые контроллером ТД требуют наличие контроллера, но некоторые могут настроены на работу без использования контроллера для этой цели.

**Контроллер БЛВС**      Большинство производителей контроллеров БЛВС производят маленькие контроллеры, которые предназначены для использования в филиалах или удаленных офисах. Когда вы проводите обследование и требуется контроллер, контроллер БЛВС для небольших офисов, который весит 907 грамм (2 фунта), будет легче и дешевле для работы, чем контроллер БЛВС уровня ядра, который весит 13,6 килограмм (30 фунтов).

**Аккумуляторные Батареи** Аккумуляторная батарея является необходимой, потому что инженер по обследованию не хочет постоянно протягивать электрический кабель, чтобы подать питание точке доступа, пока она временно установлена для обследования места. Аккумуляторная батарея не только обеспечивает питание точке доступа, она также обеспечивает более безопасную среду, потому что вам не нужно протягивать незакрепленный кабель питания по полу, и это еще позволяет просто и быстро перемещать точку доступа на новое место.

**Бинокль** Может показаться странным иметь бинокль на обследовании внутри помещений, но он может быть очень полезным в высоких складах и конференц-центрах. Они также могут быть полезны при рассматривании вещей в пространстве над потолком.

**Фонарь** Мощный направленный фонарь может оказать полезным в темном углу или на потолке.

**Рация или Сотовые Телефоны** При проведении обследования в офисной среде часто нужно вести себя тихо и по возможности незаметно. Рация или сотовые телефоны обычно более предпочтительны по сравнению с криком через всю комнату. Вы можете также вспомнить, что радиоволна является трехмерной, и это является обычным, когда один человек находится на этаже с точкой доступа, пока другой человек на другом этаже проверяет принимаемый сигнал.

**Антенны** Разнообразие всенаправленных и направленных внутренних антенн исторически были обычными предметами в наборах обследования Wi-Fi внутри помещений. Хотя внешние антенны все еще используются, их использование уже не такое распространенное как в прошлом. Большинство производителей корпоративных ТД интегрируют антенны прямо в ТД, при этом размещение и диаграмма направленности антенн разработаны для ТД, монтируемой на потолке. Если внутренние встроенные антенны не удовлетворяют потребностям вашего проекта, то у производителей ТД также есть модели ТД, которые поддерживают внешние антенны.

**Временные Монтажные Приспособления** Во время обследования места, вы будете временно крепить точку доступа—часто очень высоко, прямо под потолком. Нужно некоторого вида решение по временной установке ТД. Часто используются резинки крепления грузов или пластиковые стяжки, а также хороший старомодный скотч (клейкая лента). Штативы могут также быть использованы для временного размещения и перемещения ТД во время обследования. Мачту или штатив можно перемещать по зданию, избегая необходимости по временной установки точки доступа на стену или потолок. Рисунок 14.12 показывает профессиональный набор обследования места от ХайвРадар [HiveRadar], [www.hiveradar.com](http://www.hiveradar.com), с мачтой, которая может вытягиваться до 274 сантиметров (9 футов) в высоту. Поиск в Интернете покажет вам много профессионально произведенных наборов по обследованию в продаже, а также примеры и даже указания как собрать свой собственный набор по обследованию или штатив. Некоторые вопросы, которые вам нужно будет обдумать, включают транспортабельность или "перевозимость" комплекта, как высоко можно разместить ТД, будет ли блок самодостаточным (особенно по питанию), и простота, с которой вы можете перемещать или перевозить блок по месту проведения обследования.

**Цифровой фотоаппарат** Цифровая камера должна использоваться для записи точного местоположения расположения точки доступа. Запись этой информации визуально поможет любому, кто будет осуществлять финальную установку потом. Настройки даты/времени на фотографии может также быть полезной при просмотре фотографий позже. С невероятными возможностями по оптическому приближению,

**РИСУНОК 14.12** Переносной штатив [tripod] для обследования БЛВС

Любезно предоставлено компанией ХайвРадар [HiveRadar]



доступными на потребительских фотоаппаратах средней ценовой категории, цифровые фотоаппараты также могут быть использованы вместо бинокля. Часто камеры вашего смартфона бывает достаточно.

**Измерительное Колесо или Лазерный Измерительный Инструмент** Нужен инструмент, чтобы убедится, что точка доступа по факту достаточно близка, чтобы протянуть 100 метровый кабель до коммутационного шкафа. Помните, что 100 метровый кабель - это кабель CAT 5E или CAT 6, проложенный по кабель-каналам. Измерительное колесо или лазерный дальномер может быть использован, чтобы помочь измерить расстояние до коммутационного шкафа или для документирования расстояния от стен для монтажа ТД в большом помещении.

**Маркеры** Цветную изоленту или kleящиеся точки можно использовать, чтобы оставить отметки, где вы хотите установить точки доступа. Оставьте небольшой кусочек цветной

изоленты в том месте, где была временно смонтирована точка доступа во время обследования места. Это поможет тому, кто будет осуществлять финальную инсталляцию ТД позже.

**Лестница или Стремянка** Лестницы и/или стремянки могут быть необходимы для временной установки точек доступа под потолком. Безопасность всегда является важным вопросом при установке ТД на потолке. В Соединенных Штатах Управление по Охране Труда [Occupational Safety and Health Administration (OSHA)] предоставляет руководства по использованию лестниц. \*В России работа с лестницами и стремянками регламентируется правилами работы на высоте Приказ Минтруда России от 16.11.2020 N 782н "Об утверждении Правил по охране труда при работе на высоте"

При проведении обследования места вы должны использовать то же самое оборудование точки доступа 802.11, которое вы планируете развернуть. Помните, что каждый не похож на других и по-разному внедряет RSSI. Не рекомендуется проводить обследование по анализу покрытия, используя точку доступа одного производителя, а устанавливать оборудование совершенно другого производителя. Многие авторитетные компании по обследованию объединяют комплекты обследования от производителей, так что они могут предложить своим заказчикам разные варианты.

## Инструменты Обследования Вне Помещений

Обследования места вне помещений [outdoor site surveys] в целях обеспечения общего беспроводного доступа для пользователей на открытом воздухе становится более распространенным. Обследования на открытом воздухе проводятся с использованием внешних взаимосвязанных [mesh] точек доступа, которые обеспечивают доступ клиентским станциям на открытом воздухе. Эти обследования Wi-Fi на открытом воздухе будут использовать большую часть тех же самых инструментов, что и обследование внутри помещений, но также могут использовать устройство системы глобального позиционирования [global positioning system (GPS)], чтобы записать координаты долготы и широты. Хотя установка 802.11 на открытом воздухе может быть использована для обеспечения доступа, очень часто обсуждение обследования на открытом воздухе касается беспроводных мостов или беспроводных транзитных каналов [backhaul] для камер наблюдения или электронного мониторингового оборудования. Wi-Fi мосты находятся на уровне распределения [distribution] и используются для обеспечения беспроводного канала связи между двумя или более проводными сетями.

Требуется полностью другой набор инструментов для обследования по организации БЛВС мостов на открытом воздухе, и требуется намного больше вычислений, чтобы гарантировать стабильность канала связи по этому мосту. В начальных главах вы узнали, что вычисления, нужные при развертывании мостовых каналов связи на открытом воздухе, многочисленны, включают в себя Зону Френеля, затухание на пути в свободном пространстве, бюджет линии связи, и запас на замирание. Дополнительные вопросы для рассмотрения могут включать расчетный излучатель [intentional radiator (IR)] и ограничения эквивалентно изотропной излучаемой мощности (ЭИИМ) [equivalent isotropically radiated power (EIRP)], в соответствии с регулирующими организациями в вашей стране. Погодные условия являются еще одним главным вопросом при любом обследовании на открытом воздухе, и понадобится установить соответствующую защиту от молнии и ветра. Обследование места по организации беспроводного моста на открытом воздухе обычно требует совместных усилий двух персон. Следующий список перечисляет

инструменты, которые вы можете использовать при обследовании места на открытом воздухе:

**Топографическая Карта** Вместо плана этажа здания может понадобится топографическая карта, которая указывает возвышения(высоты) и местоположения.

**ПО по Анализу Канала Связи** Программное обеспечение по анализу канала связи точка-точка может быть использовано с топографическими картами, чтобы создать профиль мостового канала связи, а также провести много необходимых вычислений, таких как зона Френеля и ЭИИМ [EIRP]. ПО по анализу мостового канала связи является предиктивным инструментом моделирования.

**Калькуляторы** Программные калькуляторы и таблички [spreadsheets] могут быть использованы для проведения необходимых вычислений для бюджета линии связи, зоны Френеля, потерь на пути в свободном пространстве, и запасов на замирание. Еще калькуляторы могут предоставить информацию по затуханию в кабеле и коэффициенту стоячей волны по напряжению (KCBN) [voltage standing wave ratio (VSWR)]. В Упражнении 14.1, вы будете использовать калькулятор для определения затухания в кабеле.

**Данные о Максимальном Росте Дерева** Деревья являются потенциальным источником препятствий для зоны Френеля. И до тех пор, пока дерево не до конца выросло, оно скорее всего вырастет еще выше. Цепная пила - это не всегда ответ, и может быть необходимым планирование высоты антенны на основе потенциального роста дерева. Региональные или местные органы лесного или сельского хозяйства должны суметь вам предоставить необходимую информацию касательно местной листвы и какой тип роста вам ожидать.

**Бинокль** Бинокли могут помочь установить линию прямой видимости. Однако, пожалуйста, помните, что определение радиоволновой линии прямой видимости подразумевает вычисление и обеспечение прозрачности (отсутствия препятствий) зоны Френеля.

**Рация или Сотовые Телефоны** Каналы связи 802.11 типа мост могут простираться до (а иногда и превышать) милю (1,61 км). Двум инженерам по обследованию, работающим в команде, понадобится некоторое устройство для связи во время обследования.

**Генератор Сигнала и Ваттметр** Генератор сигнала может быть использован вместе с ваттметром для проверки кабеля, разъемов, и аксессуаров на затухание сигнала и KCBN [VSWR]. Эти испытательные приборы могут быть использованы для проверки кабеля и разъемов до инсталляции. Испытательные приборы также могут быть использованы после инсталляции, чтобы проверить, что вода и другие условия окружающей среды не повредили кабель и разъемы.

**Переменный Аттенюатор** Переменные аттенюаторы [variable-loss attenuator] имеют циферблат, который позволяет вам настроить количество поглощаемой энергии. Он может быть использован во время обследования места на открытом воздухе, чтобы сымитировать разные длины кабелей или потери в кабеле.

**Инклинометр** Это устройство используется для определения высоты препятствий. Выполнение этого является критичным, когда вам нужно гарантировать, что путь канала связи свободен от препятствий.

**GPS** Запись долготы и широты места передачи и любого препятствия или

**660** Глава 14 • Обследование места и Контрольное обследование интересующей точки вдоль пути является важным при планировании. GPS может легко предоставить эту информацию.

**Цифровой фотоаппарат** Вы можете захотеть сделать фотографии мест монтажа на открытом воздухе, кабельную трассу, места заземления, препятствия, и т.д. Вам вероятно нужна будет камера с хорошими линзами оптического приближения. Если у вашего фотоаппарата достаточно сильные линзы оптического приближения, вы также можете определить и задокументировать линию прямой видимости вашего канала связи. Камеры в вашем смартфоне часто бывает достаточно.

**Анализатор Спектра** Это устройство должно быть использовано, чтобы проверить окружающие радио уровни на передающей стороне, вместе с определением возможных источников радиоинтерференции

**Фонарь-Прожектор или Отражатель Солнечного Света** В случае беспроводного моста, вам нужно будет убедиться, что вы проводите обследование в правильном направлении. По мере удаления дальше и дальше, определить конкретную крышу или башню становится труднее и труднее. Чтобы помочь в этой задаче, может использоваться мощный (3 миллиона свечей (кандел) или больше) фонарь или отражатель солнечных лучей. Так как свет распространяется очень хорошо, то его можно использовать для фокусирования в реальное удаленное место, чтобы убедится, что обследование проводится в правильном направлении.

Антенны и точки доступа обычно не используются во время обследования места для организации моста. Оборудование для организации моста редко устанавливается во время обследования, потому что в большинстве требуется строительство мачты или другого типа конструкции. Если измерения для организации моста точны, то канал связи типа мост скорее всего будет работать. Обследование места на открытом воздухе для взаимосвязанной [mesh] сети требует наличие ТД и антенн.

## УПРАЖНЕНИЕ 14.1

### Вычисление Затухания(Потерь) в Кабеле

Чтобы выполнить это упражнение, вы должны зайти на вебсайт Таймз Макровейв [Times Microwave] ([www.timesmicrowave.com](http://www.timesmicrowave.com)). На веб-сайте найдите ссылку на Калькулятор Коаксиального Кабеля [Coaxial Cable Calculator]. На момент перевода это ссылка Calculator.

1. В поле выбора серии продукта [Product Family] выберите LMR, в поле выбора Кабеля [Cable] выберите кабель класса LMR-1200-DB.
2. В поле Частота [Frequency (MHz)], введите **2500**, а в поле Длина [Run Length (ft)] (Футы), введите **200** футов.
3. Нажмите кнопку Вычислить [Calculate].

Отметьте количество потерь дБ на 100 футов [dB/100 ft] или дБ на 100 метров [dB/100m] для этого кабеля.

4. В поле выбора кабеля выберите кабель более низкого класса - LMR-400.
5. В поле Частота [Frequency (MHz)], введите **2500**, а в поле Длина [Run Length (ft)] (Футы), введите **200** футов.
6. Нажмите кнопку Вычислить [Calculate].

Обратите внимание, что для этого класса кабеля на много выше потери дБ на 100 футов и дБ на 100 метров соответственно.

# Документы и Отчеты

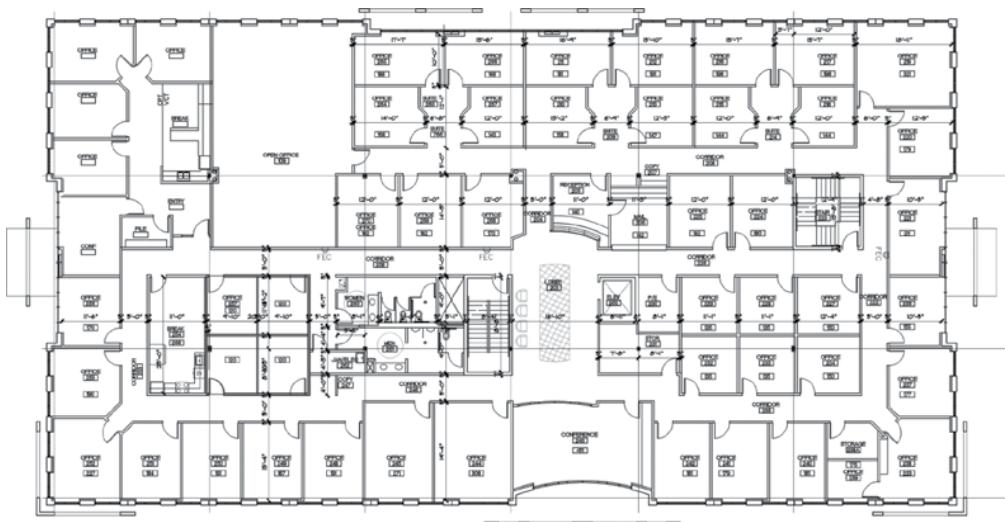
Во время интервью о проекте БЛВС (и до обследования места) вы должны получить надлежащую документацию о физическом объекте и сети. Дополнительно, вы должны создать контрольные списки обследования места и следовать ему во время физического обследования. После того, как проведено физическое обследование, вы должны предоставить профессиональный и исчерпывающий итоговый отчет заказчику. Дополнительные отчеты и рекомендации заказчику также могут быть включены в итоговый отчет. Этот отчет должен предоставлять детальные инструкции по тому как устанавливать и настраивать предлагаемую сеть таким образом, чтобы любой мог прочитать отчет и понимать ваш замысел.

## Бланки и Документация Заказчика

Перед интервью при обследовании места вы должны получить следующие критически важные документы от заказчика:

**Чертежи** Вам нужен развернутый план этажа для того, чтобы обсуждать потребности в покрытии и емкости с сетевым административным персоналом. Как обсуждалось ранее в этой главе, при просмотре поэтажных планов, держите в уме, что требования по емкости и покрытию нужно запланировать заранее. Необходимо также сделать фотокопии плана этажа, и использовать их для записи радио измерений, которые проводятся во время физического обследования места, а также для записи о местах размещения оборудования. Некоторые программные инструменты по обследованию позволяют вам импортировать поэтажные планы, и программа будет записывать результаты обследования на план этажа за вас. Рисунок 14.13 показывает пример типового плана этажа. Чертежи настоятельно рекомендуются и значительно облегчают составление итогового отчета.

**РИСУНОК 14.13** Типовой план этажа



Что, если у заказчика не комплекта чертежей? Чертежи могут быть найдены в различных местах. У архитектора здания вероятно всё ещё будут храниться копии чертежей. Многие планы этажей общественных и частных зданий могут также быть найдены в общественных государственных местах, например в городском совете, администрации города или подразделении МЧС, пожарном

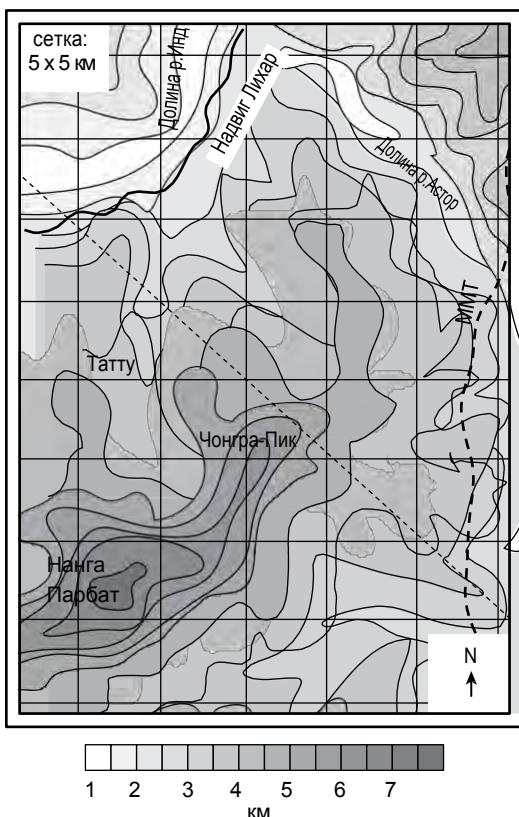
департаменте. Предприятия обычно обязаны размещать план эвакуации при пожаре. Многие обследования мест были проведены с использованием простого пожарного плана эвакуации, нарисованного в масштабе, если чертежи не могли найти.

В худшем случае, вы можете использовать миллиметровку (бумага с миллиметровой сеткой) и нарисовать план этажа вручную. Инструменты предиктивного анализа требуют детальную информацию о материалах здания, которые можно найти на чертежах.

Чертежи могут уже быть в формате векторной графики (DWG и DWF) для импортирования в приложение предиктивного анализа, или их можно отсканировать.

**Топографическая Карта** Если планируется обследование на открытом воздухе, то может понадобится топографическая карта, также называемая *контурной картой* [*contour map*]. Контурные карты отображают информацию о местности, такую как возвышения, лесные массивы, и расположение потоков воды или водоемов. Рисунок 14.14 изображает типовую топографическую карту. Топографическая карта будет нужна, когда вы проводите расчеты для организации моста, например чистоту зоны Френеля.

**РИСУНОК 14.14** Топографическая карта



**Карта Топологии Сети** Понимание схемы текущей проводной сетевой инфраструктуры ускорит процесс обследования и позволит лучше спланировать БЛВС на этапе проектирования. Карта топологии компьютерной сети предоставляет необходимую информацию, такую как местоположение коммутационных шкафов и границы Зего уровня. Топология БЛВС будет интегрирована на столько бесшовно, насколько это возможно в проводную инфраструктуру. VLANы обычно используются для сегментации и проводной и беспроводной сетей.

Получение карты сетевой топологии от заказчика является очень рекомендуемой практикой, которая поможет создать хорошо спроектированную и правильно интегрированную БЛВС. Некоторые организации не желают раскрывать свои проводные сетевые топологии в целях безопасности. Может понадобится получать разрешение от служб безопасности [security clearance] и/или подписывать соглашение о неразглашении [nondisclosure agreements], чтобы получить доступ к этим документам.

**Пропуска и разрешения** Вам может понадобится соответствующее разрешение от охраны по доступу к помещениям при проведении обследования места. Больницы, государственные учреждения, и многие предприятия требуют наличие бэджа, пропуска и сопровождения для входа на определенные территории. Понадобится встреча с персоналом по безопасности и/или ответственным за помещения до обследования, для того чтобы выполнить все требования по физической безопасности. Вы не захотите появиться на объекте заказчика и быть отправленным обратно до следующего раза, потому что кто-то забыл забронировать сопровождение охраны. Независимо от требований по безопасности, всегда является хорошей идеей, чтобы сетевой администратор предупредил всех, что вы будете на объекте.

Как профессионал по обследованию и проектированию БЛВС, вы создадите свою собственную документацию или необходимые контрольные списки, которые будут использоваться во время интервью и во время реального физического обследования. Вот несколько типов контрольных списков по обследованию и проектированию:

**Контрольный список интервью** Подробный контрольный список [checklist] содержит все вопросы, которые нужно задать во время интервью при обследовании места, должен быть создан заранее. Многие уточняющие вопросы для интервью, обсужденные ранее в этой главе, будут присутствовать в контрольном списке интервью.

**Контрольный список установки** Многие профессионалы по обследованию предпочитают записывать детали установки на документах плана этажа. Установочный контрольный список, детализирующий размещение и монтаж оборудования для каждой отдельной точки доступа, также является опцией. Может быть записана информация о положении ТД, типе антенны, ориентации антенны, монтажных устройств, и источников питания.

**Контрольный список оборудования** Для организационных целей контрольный список всего оборудования и программных инструментов, используемых во время обследования, может также быть хорошей идеей. Все необходимые инструменты для обследований внутри помещений и на открытом воздухе описаны в этой главе.

## Представляемые результаты

После того как процесс интервью завершен, а обследование места проведено, заказчику должен быть передан итоговый отчет [final report]. Информация, собранная во время обследования места, должна быть организована и сформирована в профессиональный технический отчет для просмотра заказчиком. Собранныя информация, содержащаяся в предоставляемых материалах, будет содержать следующее:

**Формулировка Цели [Purpose Statement]** Итоговый отчет должен начинаться с

**664** Глава 14 • Обследование места и Контрольное обследование формулировки цели БЛВС, которая указывает требования заказчика и бизнес-обоснование для БЛВС.

**Анализ Спектра [Spectrum Analysis]** Обязательно определите потенциальные источники интерференции.

**Анализ радио-покрытия [RF Coverage Analysis]** Определите границы зоны радиоприема.

**Размещение и Настройка Оборудования** Рекомендуемые места размещения ТД, ориентация антенн, модель переиспользования каналов, настройки мощности, и любую другую специфичную для ТД информацию, такую как способ установки и прокладка кабеля.

**Анализ Емкости и Производительности** Включите результаты из тестов пропускной способности приложений, которые иногда являются опциональным аналитическим отчетом, входящим в итоговый отчет об обследовании.

Подробный отчет об обследовании места может содержать сотни страниц, в зависимости от размера объекта. Отчет об обследовании часто включает в себя фотографии, которые делались цифровым фотоаппаратом во время обследования. Фотографии могут использоваться для фиксации размещения ТД, и идентификации проблем, таких как интерферирующие радиоустройства, или потенциальные проблемы для установки, такие как твердый потолок или бетонные стены. Существует профессиональное программное обеспечение по обследованию мест, которое генерирует отчеты профессионального качества, используя подготовленные шаблоны.

## Дополнительные Отчеты

Вместе с отчетом об обследовании, могут быть выданы другие рекомендации для того, чтобы установить соответствующее оборудование и безопасность. Обычно, индивидуальных предпринимателей и/или компании, которые проводят обследование места, также нанимают на установку беспроводной сети. Однако, заказчик может использовать информацию из отчета об обследовании, чтобы провести свою собственную установку. Независимо от того, кто проводит установку, другие рекомендации и отчеты будут предоставлены вместе с отчетом об обследовании:

**Рекомендации по Производителям** На рынке присутствует много беспроводных производителей. Настоятельно рекомендуемая практика - проводить обследование объекта с использованием оборудования того же производителя, который будет поставлять оборудование, которое будет в дальнейшем развернуто на объекте. Хотя IEEE устанавливает стандарты для обеспечения совместимости, оборудование каждого производителя Wi-Fi работает в некотором роде в собственной манере. Например, каждый производитель БЛВС использует свой собственный протокол адаптивного радио [adaptive RF protocol]. Простой факт того, что радиомодули каждого производителя используют собственные пороги RSSI является достаточной причиной, чтобы использовать того же самого производителя во время обследования и инсталляции. Многие профессионалы по обследованиям мест имеют наборы разных производителей для работы по обследованию. Это не необычно для компаний по обследованиям провести два обследования с оборудованием двух разных производителей, и представить заказчику два разных варианта. Однако, процесс интервью обычно заранее определяет рекомендации по производителям, которые будут даны заказчику.

**Схемы Установки** На основе собранной информации во время обследования места заказчику будет представлена итоговая схема проекта. Схема установки это по сути карта топологии беспроводной сети, которая иллюстрирует, где будут установлены точки доступа и как беспроводная сеть будет интегрирована с существующей проводной инфраструктурой. Обычно даются ясные определения размещения ТД, VLANов, и границ Зего уровня.

**Ведомость Материалов** Вместе со схемами установки предоставляется подробная ведомость материалов [*bill of materials (BOM)*], которая перечисляет все аппаратные и программные компоненты, необходимые для итоговой установки беспроводной сети. Указывается номер модели и количество каждой части оборудования. Туда входят точки доступа, мосты, беспроводные контроллеры, антенны, разъемы, и грозозащитники.

**График и Затраты Проекта** Должен быть подготовлен предварительный подробный график установки, который выделяет все временные линии, стоимость оборудования, и трудозатраты. Особое внимание должно быть уделено зависимостям в графике, таким как время доставки и лицензирования, если это применимо.

**Рекомендации по Решениям по Безопасности** Как упоминалось ранее в этой главе, ожидания по безопасности должны быть обсуждены во время интервью на обследование места. На основе этих обсуждений, компания по обследованию дает исчерпывающие рекомендации по беспроводной безопасности. Все аспекты аутентификации, авторизации, учета [*accounting*], шифрования и сегментации должны быть включены в документацию с рекомендациями по безопасности.

**Рекомендации по Беспроводной Политике** Дополнение к рекомендациям по безопасности могут быть рекомендации по корпоративной беспроводной политике. Вам возможно понадобится помочь заказчику в написании политики по безопасности беспроводной сети, если у него ее еще нет.

**Рекомендации по Обучению** Одна из наиболее часто пропускаемых областей при развертывании новых решений - это соответствующее обучение. Настоятельно рекомендуется сетевому персоналу заказчика записаться на курсы по администрированию и безопасности беспроводной сети. Кроме того, должны быть запланированы краткие курсы для всех конечных пользователей.

## ИТОГО

В этой главе вы узнали о предварительной подготовке и вопросах, которые обязательно нужно спросить до проведения беспроводного обследования места. Интервью по обследованию и проекту БЛВС является важным процессом, который необходим и для обучения заказчика и для определения беспроводных потребностей заказчика. Определение бизнес цели беспроводной сети ведет к более продуктивному обследованию. Планирование емкости и покрытия, а также планирование подключения к инфраструктуре, все являются частями обследования и интервью по проекту БЛВС. До интервью вы должны получить критически важную документацию от заказчика, такую как чертежи или топографические карты. Контрольные списки для интервью и инсталляции используются в время интервью

**666** Глава 14 • Обследование места и Контрольное обследование по обследованию и во время физического обследования. Для разных вертикальных рынков требуются разные вопросы для обследования.

Вы также узнали об обязательных и optionalных аспектах беспроводного обследования. Мы обсудили значимость обнаружения потенциальных источников интерференции с использованием анализатора спектра, и мы определили шаги, которые необходимо провести как ручным и пассивным обследованием по анализу покрытия, так и проведение предиктивного обследования.

Эта глава также предоставляет доклад о необходимых инструментах для обследования как внутри помещений так и на открытом воздухе. После установки, требуется контрольное обследование и подтверждение, что ваш запланированный проект работает так, как ожидалось.

После того как обследование завершено, вы должны предоставить заказчику итоговый отчет об обследовании, а также дополнительные отчеты и рекомендации.

# Темы Экзамена

**Дать определение интервью по обследованию места.** Уметь объяснить важность процесса интервью до беспроводного обследования. Понимать, что интервью является обучением заказчика и четким определением всех его беспроводных потребностей.

**Определить вопросы, необходимые для определения потребностей по емкости и покрытию.** Понимать значимость надлежащего планирования емкости и покрытия. Определить все многочисленные вопросы для обсуждения при планировании радиопокрытия, полосы и пропускной способности.

**Определить вопросы с подключением к инфраструктуре.** Понимать все необходимые вопросы, которые должны быть заданы для того, чтобы гарантировать надлежащую интеграцию БЛВС в существующую проводную инфраструктуру.

**Определить источники интерференции с БЛВС.** Описать все разнообразные устройства, которые являются потенциальными источниками интерференции в полосах 2,4 ГГц ISM и 5 ГГц U-NII.

**Понимать разные методологии обследования места.** Понимать разницу между методом ТД-на-палке и гибридным методом, который основан на предиктивном моделировании.

**Объяснить радио измерения.** Уметь объяснить процедуру, используемую при проведении анализа покрытия, и разные типы записываемых радиоизмерений, включая силу принимаемого сигнала и отношение сигнал-шум.

**Определить все инструменты по обследованию места.** Понимать разницу между обследованиями на открытом воздухе и внутри помещений, и определять все необходимые инструменты.

**Объяснить два типа анализа покрытия.** Описать разницу между ручным и предиктивным обследованиями, и объяснить технологию самоорганизующейся БЛВС.

**Понимать значение проведения контрольного обследования беспроводной сети.** Объяснить значение проверки беспроводной сети для подтверждения только что установленной сети или помощи в поиске и устранении проблем на сети, которая работает не так как ожидалось.

**Определить документацию и формы по обследованию места.** Определить всю документацию, которая должна быть подготовлена и собрана до обследования места. Знать всю информацию и документацию, которая нужна в итоговых предоставляемых материалах.

**Объяснить обсуждаемые вопросы для вертикальных рынков.** Понимать бизнес требования разных вертикальных рынков, и как эти требования будут видоизменять обследования и итоговую инсталляцию.

# Контрольные Вопросы

1. Какое из следующих выражений лучше описывает вопросы безопасности во время беспроводного обследования места? (Выберите все, что применимо.)
  - A. Вопросы будут заданы, чтобы определить ожидания заказчика по безопасности.
  - B. Рекомендации по беспроводной безопасности будут выданы после обследования.
  - C. Рекомендации о политике беспроводной безопасности также могут быть сделаны.
  - D. Во время обследования должны быть включены и взаимная аутентификация, и шифрование.
2. Больница АКМЕ использует телеметрическую мониторинговую систему на основе поддержки соединения в отделении кардиологической помощи. Руководство хочет, чтобы приложение было доступно по БЛВС. Время непрерывной работы [uptime] является очень важным из-за критичной природы системы мониторинга. На что должен смотреть инженер по обследованию и проектированию что может вызвать потерю связи по БЛВС? (Выберите все, что применимо.)
  - A. Интерференция медицинского оборудования
  - B. Защитное стекло, содержащее сетку из металлической проволоки
  - C. Пациенты
  - D. Подкладное судно
  - E. Лифтовые шахты
3. Какой из перечисленных инструментов может быть использован на обследовании на открытом воздухе области, предназначенной для обеспечения покрытия на открытом воздухе? (Выберите все, что применимо.)
  - A. Анализатор Спектра [Spectrum analyzer]
  - B. Чертежи или топографическая карта местности [Outdoor blueprints or topography map]
  - C. Взаимосвязные маршрутизаторы [Mesh routers]
  - D. GPS
  - E. Осциллограф [Oscilloscope]
4. Название уникального вопроса при развертывании беспроводной сети в гостинице или другом предприятии сферы гостеприимства. (Выберите лучший ответ.)
  - A. Кража оборудования [Equipment theft]
  - B. Эстетика [Aesthetics]
  - C. Сегментация [Segmentation]
  - D. Роуминг [Roaming]
  - E. Управление пользователями [User management]
5. Какой документ может быть нужен до проведения обследования внутри помещения для новой беспроводной ЛВС? (Выберите все, что применимо.)
  - A. Чертежи [Blueprints]
  - B. Топографическая карта сети [Network topography map]

- C. Карта топологии сети [Network topology map]
  - D. Карта покрытия [Coverage map]
  - E. Карта частот [Frequency map]
6. После проведения простого обследования места в офисном здании, где ваша компания находится на пятом этаже, вы обнаружили, что у других компаний также работают точки доступа на соседних этажах на каналах 2 и 8. Какую лучшую рекомендацию вы дадите руководству относительно развертывания новой БЛВС для вашей компании?
- A. Установить 2,4 ГГц точку доступа на канале 6 и использовать самые высокие доступные настройки мощности, чтобы мощность БЛВС была выше чем у других компаний.
  - B. Поговорить с другими компаниями. Предложить им использовать каналы 1 и 6 с более низкими настройками мощности. Установить 2,4 ГГц точку доступа с использованием канала 9.
  - C. Поговорить с другими компаниями. Предложить им использовать каналы 1 и 11 с более низкими настройками мощности. Установить 2,4 ГГц точку доступа с использованием канала 6.
  - D. Рекомендовать установку ТД с 5 ГГц радиомодулями.
  - E. Установить беспроводную систему предотвращения проникновения [wireless intrusion prevention system (WIPS)]. Классифицировать точки доступа других компаний как мешающие и применить деаутентификационные контрмеры.
7. Корпорация Дюарте наняла вас для получения рекомендаций о будущем развертывании беспроводной сети, которая требует более 300 точек доступа, чтобы выполнить все требования по покрытию. Какая наиболее эффективная по стоимости и практичная рекомендация в отношении обеспечения электропитания для точек доступа?
- A. Рекомендуется, чтобы заказчик заменил старые пограничные коммутаторы на новые со встроенным PoE.
  - B. Рекомендуется, чтобы заказчик заменил коммутатор ядра на новый коммутатор ядра со встроенным PoE.
  - C. Рекомендуется, чтобы заказчик использовал однопортовые инжекторы питания.
  - D. Рекомендуется, чтобы заказчик нанял электрика для установки новых электрических розеток.
8. Во время процесса интервью, какие темы будут обсуждаться для того, чтобы БЛВС надлежащим образом была интегрирована в существующую проводную архитектуру?
- A. PoE
  - B. Сегментация [Segmentation]
  - C. Управление Пользователями [User management]
  - D. Управление ТД [AP management]
  - E. Все выше перечисленное
9. Региональная больница округа Митчелл наняла вас для беспроводного обследования места. До проведения обследования вы должны проконсультироваться с сотрудниками из каких департаментов? (Выберите все, что применимо.)
- A. Отдел сетевых администраторов [Network management]
  - B. Отдел технического обслуживания медицинской техники [Biomedical department]

- C. Охрана больницы [Hospital security]
  - D. Административно-Хозяйственная Часть [Custodial department]
  - E. Отдел Маркетинга [Marketing department]
10. Какую дополнительную документацию обычно предоставляют вместе с итоговыми материалами, передаваемыми заказчику, по обследованию? (Выберите все, что применимо.)
- A. Ведомость Материалов [Bill of materials]
  - B. Схемы установки [Implementation diagrams]
  - C. Таблицы потребления питания [Power consumption charts]
  - D. График и затраты проекта [Project schedule and costs]
  - E. Руководства пользователя точки доступа [Access point user manuals]
11. Какой тип анализа покрытия требует, чтобы радио карта была ассоциирована с точкой доступа?
- A. Ассоциированный
  - B. Пассивный
  - C. Предиктивный
  - D. Вспомогательный
  - E. Активный
12. Какой из следующих инструментов может быть использован при обследовании внутри помещений? (Выберите все, что применимо.)
- A. Измерительное колесо
  - B. GPS
  - C. Лестница
  - D. Аккумуляторная батарея
  - E. Микроволновая печь
13. Наименование потенциальных источников интерференции в 5 ГГц полосах U-NII. (Выберите все, что применимо.)
- A. Микроволновые печи
  - B. Беспроводные телефоны
  - C. FM радиоприемник
  - D. Радар
14. Какое из этих измерений проводится во время пассивного ручного обследования сайта? (Выберите все, что применимо.)
- A. SNR
  - B. дБи [dBi]
  - C. сила сигнала в дБм [dBm signal strength]
  - D. дБд [dBd]

- 15.** Название потенциальных источников интерференции, которые можно обнаружить во время обследования места в 2,4 ГГц. (Вы берите все, что применимо.)
- A.** Тостеры [Toaster ovens]
  - B.** Плазменные резаки [Plasma cutters]
  - C.** Bluetooth наушники [Bluetooth headsets]
  - D.** Видео камеры 2,4 ГГц [2.4 GHz video cameras]
- 16.** Какие настройки точки доступа должны быть записаны во время обследования ТД-на-палке? (Выберите все, что применимо.)
- A.** Настройки мощности [Power settings]
  - B.** Настройки шифрования [Encryption settings]
  - C.** Настройки аутентификации [Authentication settings]
  - D.** Настройки канала [Channel settings]
  - E.** IP адреса [IP addresses]
- 17.** Какой тип обследования использует моделирующие алгоритмы и значения затуханий, чтобы создать визуальную модель радиопокрытия?
- A.** Ассоциированный [Associated]
  - B.** Пассивный [Passive]
  - C.** Предиктивный [Predictive]
  - D.** Вспомогательный [Assisted]
  - E.** Активный [Active]
- 18.** Корпорация АКМЕ наняла вас для проектирования беспроводной сети, в которой будут клиенты с передачей данных, телефоны VoWiFi, которые не поддерживают 802.11g, и доступ для гостевых пользователей. Компания хочет самое сильное возможное решение по безопасности для клиентов с передачей данных и телефонов. Какой дизайн лучше всего подходит под требования заказчика?
- A.** Создать один беспроводной VLAN. Отделить клиентов с передачей данных, телефоны VoWiFi и гостевых пользователей от проводной сети. Использовать аутентификацию 802.1X/EAP и шифрование CCMP/AES для решения по беспроводной безопасности.
  - B.** Создать три отдельных VLANa. Разделить клиентов с передачей данных, телефоны VoWiFi и гостевых пользователей по трем разным VLANам. Использовать аутентификацию 802.1X/EAP и шифрование TKIP для безопасности в VLANe данных. Использовать WPA2-Personal в голосовом VLANe. Гостевой VLAN будет без безопасности, кроме может быть перехватывающего портала [captive portal].
  - C.** Создать три отдельных VLANa. Разделить клиентов с передачей данных, телефоны VoWiFi, и гостевых пользователей по трем разным VLANам. Использовать аутентификацию 802.1X/EAP с шифрованием CCMP/AES для безопасности в VLANe данных. Использовать WPA2-Personal в голосовом VLAN. Трафик гостевого VLAN будет требовать перехватывающий веб портал [captive web portal] и политику межсетевого экрана для безопасности.
  - D.** Создать два отдельных VLANa. Клиенты с передачей данных и голосовые клиенты будут в одном VLANе, а гостевые пользователи будут в другом. Использовать аутентификацию 802.1X/EAP и шифрование CCMP/AES для безопасности VLANa данных и голоса. Гостевой VLAN без безопасности, кроме может быть перехватывающего портала [captive portal].

- 19.** Какой тип обследования БЛВС является наиболее важным обследованием, которое должно всегда выполняться независимо от того в каком вертикальном рынке происходит установка?
- A.** Обследование ТД-на-палке [AP-on-a-stick survey]
  - B.** Гибридное обследование [Hybrid survey]
  - C.** Предиктивное моделирующее обследование [Predictive model survey]
  - D.** Контрольное обследование [Validation survey]
- 20.** Наименование необходимых вычислений при обследовании по организации моста на открытом воздухе до 5 миль ( 8 км). (Выберите все, что применимо.)
- A.** Бюджет линии связи [Link budget]
  - B.** Потери на пути в свободном пространстве [Free space path loss]
  - C.** Зона Френеля [Fresnel zone]
  - D.** Настройка запаса на замирание [Fade margin adjustment]
  - E.** Высота ширины луча антенны [Height of the antenna beamwidth]

# Глава 15



## Решение проблем БЛВС

---

В ЭТОЙ ГЛАВЕ ВЫ УЗНАЕТЕ О СЛЕДУЮЩЕМ:

✓ **Пять принципов решения проблем БЛВС**

- Передовой опыт решения проблем
- Решение проблем по модели OSI
- Большинство проблем с Wi-Fi являются проблемами с клиентом
- Надлежащий проект БЛВС уменьшает количество проблем
- БЛВС всегда виноват

✓ **Решение проблем на Уровне 1**

- Проект БЛВС
- Мощность передачи
- Радиоинтерференция
- Драйверы
- PoE
- Ошибки в прошивке

✓ **Решение проблем на Уровне 2**

- Повторные передачи Уровня 2
- Радиоинтерференция
- Низкий SNR
- Интерференция смежных каналов
- Скрытый узел
- Несовпадающая мощность
- Многолучевое распространение



✓ **Решение проблем безопасности**

- Решение проблем с PSK
- Решение проблем с 802.1X/EAP
- Решение проблем с VPN

✓ **Решение проблем роуминга**

✓ **Утилизация канала**

✓ **Решение проблем 3-7 Уровней**

✓ **Инструменты решения проблем БЛВС**

- Приложения по обнаружению БЛВС
- Анализаторы спектра
- Анализаторы протоколов
- Инструменты проверки пропускной способности
- Стандартные проверочные утилиты IP сети
- Безопасная оболочка [Secure Shell]



Из этой книги вы узнали о строительных блоках основ БЛВС. Как и с любым типом сети связи, однако, могут возникать проблемы с сетями БЛВС, которые могут

потребовать внимание администратора. Часто возникающие проблемы с клиентским подключением могут быть результатом неправильного внедрения безопасности БЛВС. Из этой главы вы узнаете о передовом опыте решения проблем и как фокусироваться на 1ом уровне и 2ом уровне при исследовании проблем Wi-Fi. Умение исследовать проблемы роуминга, а также мониторить утилизацию канала является ключевым в поддержке хорошего состояния БЛВС. Вы также узнаете о стратегиях решения проблем БЛВС с точки зрения безопасности. Хотя эта глава не подразумевает под собой пошаговое диагностическое руководство, но из нее вы узнаете о многих распространенных проблемах БЛВС и предлагаемых решениях. Мы также обсудим много бесплатных и коммерческих инструментов по решению проблем БЛВС, которые имеются в наличии.

## Пять Принципов Решения Проблем БЛВС

Прежде, чем мы обсудим конкретные стратегии решения проблем БЛВС, вы должны понимать следующие пять принципов для решения любого типа проблемы БЛВС:

- Применение передового опыта решения проблем.
- Решение проблем по модели OSI.
- Большинство проблем находится на клиентской стороне.
- Надлежащее проектирование/планирование БЛВС является важным.
- Всегда будут винить БЛВС.

Теперь мы рассмотрим эти доктрины по решению проблем БЛВС более подробно.

### Передовой опыт решения проблем

Основы передового опыта решения проблем - это задавать вопросы и собирать информацию. Во время решения проблем компьютерной сети любого типа вы должны спросить корректные вопросы, чтобы собрать информацию, которая относится к проблеме. Очень просто отклониться в сторону при решении проблем, так правильные вопросы помогут ИТ администратору сфокусироваться на относящихся к делу данных с целью изоляции основной причины проблемы. Например, проблемы в безопасности БЛВС часто приводят к проблемам с подключением у клиентов БЛВС; постановка соответствующих вопросов укажет

вам правильное направление в решении проблемы. Следующие базовые вопросы являются одними из тех, что нужно спросить:

- Когда происходит проблема?

В какое время случилась проблема? Происходит ли проблема во время четко определенного периода времени? Эта информация может быть легко определена путем просмотра лог-файлов [log files] ТД, контроллеров БЛВС, и применяемых серверов, например, RADIUS. Передовой опыт предписывает, чтобы все *Сетевые Протоколы Времени* [Network Time Protocol (NTP)] и настройки временной зоны были корректно настроены на всем сетевом оборудовании.

- Где происходит проблема?

Проблема повсеместна или она существует только в одном физическом месте? Проблема происходит на одном этаже или по всему зданию? Проблема влияет только на одну точку доступа или на группу точек доступа? Определение местоположения проблемы поможет вам собрать лучше информацию в направлении решения проблемы.

- Проблема влияет на одного клиента или на несколько клиентов?

Если проблема влияет только на одного клиента, у вас может быть просто проблема с драйвером или неправильно настроенной программой аутентификации на клиенте. Если проблема влияет на несколько клиентов, то проблема очевидно является большим вопросом. Большинство проблем с подключением находится на стороне клиента, досаждают ли они одному клиенту или нескольким клиентам.

- Проблема повторяется или она произошла всего лишь один раз?

Решение проблемы, которая случилась только один раз или несколько раз, может быть трудным. Сбор данных намного проще для повторяющихся проблем. Вы можете включить отладочные команды [debug commands] на ТД или контроллерах БЛВС в надежде снова поймать проблему в лог-файл [log file].

- Делали ли вы какие-либо изменения недавно?

Это является вопросом, который всегда задает персонал поддержки производителя БЛВС своим заказчикам. А ответом почти всегда является - нет, даже не смотря на тот факт, что изменения на сети имели место быть. Передовой опыт диктует, что любые изменения настроек сети должны прорабатываться и планироваться по времени. Логи (журналы) аудита безопасности инфраструктуры БЛВС всегда оставляют след того, какой администратор какие изменения сделал в любое определенное время.

Задав многочисленные вопросы, вы можете начать процесс решения проблемы.

Передовой опыт решения проблем включает следующее:

- 1. Определение проблемы.**

Так как всегда кажется, что виноват БЛВС, то это даже более важно корректно идентифицировать проблему. Определить, что проблема действительно существует. Постановка вопросов и сбор информации поможет вам определить настоящую проблему.

- 2. Воссоздание проблемы.**

Наличие возможности повторить проблему на месте или в удаленной лаборатории позволит вам собрать больше информации для диагностики проблемы. Если вы не можете воссоздать проблему, вам нужно задать больше вопросов.

**3. Локализация и изоляция причины.**

Весь смысл в спрашивании наводящих вопросов и сборе данных в том, чтобы вы могли изолировать основную причину проблемы. Решение проблемы по модели OSI также поможет вам определить виновника. Определите находится ли проблема на уровне доступа, уровне распределения или в ядре вашего сетевого дизайна.

**4. Решение проблемы.**

Сформулируйте и примените план по решению проблемы. Это может потребовать изменений на сети, обновлении прошивки, и т.д.

**5. Проверочное тестирование для подтверждения, что проблема решена.**

Всегда обязательно тестируйте в разных местах в разное время и несколькими устройствами. Расширенная проверка гарантирует, что проблема действительно решена.

**6. Документирование проблемы и решения.**

Передовой опыт решения проблем предписывает, чтобы вы документировали все проблемы, диагностику и решения. Справочная база данных службы поддержки поможет вам в своевременном решении проблем, если проблема повторится.

**7. Предоставление обратной связи.**

В качестве профессионального этикета всегда обязательно связывайтесь с человеком (людьми), кто первыми оповестили вас о проблеме и сообщите о решении проблемы.

## Решение проблем по модели OSI

Тот же самый диагностический подход, используемый для решения проблем проводных сетей 802.3, должен быть применим при решении проблем беспроводной локальной вычислительной сети (БЛВС) [wireless local area network (WLAN)]. Подход снизу-вверх для анализа уровней сетевой модели OSI также применим к беспроводным сетям.

Помните, что технология 802.11 похожа на 802.3, в которой она работает на первых двух уровнях модели OSI. По этой причине, администратору БЛВС стоит всегда пытаться сначала определить присутствует ли проблема на уровне 1 и уровне 2. Если первые два уровня модели OSI исключены в качестве причины проблемы, то проблема не является Wi-Fi проблемой, и должны быть исследованы более высокие уровни модели OSI.

Как и с большинством сетевых технологий, большинство проблем обычно находится на Физическом уровне. Простые проблемы уровня 1, такие как не запитанные точки доступа или проблемы с драйвером клиентского радиомодуля, часто являются причиной проблем с подключением или производительностью. Сбой в распространении радиосигнала и радиоинтерференция влияют и на производительность, и на покрытие вашей БЛВС. Несоответствующее покрытие БЛВС, емкость и производительность часто являются проблемами уровня 1, которые являются результатом слабого дизайна БЛВС. Проблемы с клиентскими драйверами и неправильными настройками программ входа в БЛВС также являются распространенными проблемами уровня 1.

После исключения уровня 1 как источника проблемы, администратор БЛВС должен определить находится ли проблема на Канальном [Data-Link] уровне. Базовая связь 802.11, такая как обнаружение, аутентификация, ассоциация, и роуминг, происходит на MAC подуровне уровня 2. Как показано на Рисунке 15.1, механизмы безопасности БЛВС также работают на уровне 2. Современные радиомодули 802.11 используют шифрование CCMP, которое обеспечивает конфиденциальность данных для уровней 3-7.

Выбранный метод шифрования должен совпадать и на ТД и на клиентском радиомодуле. Например, если на ТД отключена обратная совместимость с шифрованием TKIP, устаревшие клиенты, которые поддерживают только TKIP не смогут подключиться. Помните, что только шифрование CCMP может быть использовано для скоростей передачи данных 802.11n (HT), 802.11ac (VHT), и 802.11ax (HE). Точка доступа может быть настроена на передачу SSID, которая поддерживает оба шифрования и TKIP и CCMP. В этой ситуации, типовой звонок в поддержку может быть таким, что устаревшие клиенты TKIP кажутся медленными из-за отсутствия поддержки более высоких скоростей передачи данных. Простое решение - это заменить устаревшие клиенты на сегодняшние клиенты с поддержкой CCMP.

**РИСУНОК 15.1** Модель OSI



В Главе 17 "Архитектура Сетевой Безопасности 802.11" вы узнаете, что существует симбиотическая связь между созданием динамических ключей шифрования и аутентификацией. *Парный главный ключ* [*pairwise master key (PMK)*] используется для обмена 4x Сторонним Рукопожатием [*4-Way Handshake*], которое генерирует динамические ключи шифрования, используемые любыми двумя радиомодулями 802.11. Парный главный ключ [PMK] создается как побочный продукт или 802.1X/EAP, PSK, или аутентификацией SAE. Следовательно, если аутентификация не проходит, то никакие ключи шифрования не создаются. Мы обсудим решение проблем обоих методов аутентификации 802.11 позже в этой главе.

Как говорилось ранее, если два первых уровня модели OSI исключены, то проблема не является Wi-Fi проблемой, а, следовательно, проблема присутствует на уровнях 3-7. Наиболее вероятно, проблема является или проблемой сети TCP/IP или проблемой приложения. Как показано на Рисунке 15.1, проблемы TCP/IP должны исследоваться на уровнях 3-4, в то время как большинство проблем с приложениями находится между уровнями 5 и 7.

## Большинство Wi-Fi проблем являются проблемами с клиентом

Как ранее упоминалось, когда бы вы не решали проблемы с БЛВС, вы должны начать с Физического уровня. Кроме того, в 70 процентах случаев проблема будет находиться на стороне Wi-Fi клиента. Если существуют какие-либо проблемы с подключением клиента, то базовое решение проблем Wi-Fi [Wi-Fi Troubleshooting 101] предписывает, чтобы вы выключили и заново включили сетевой адаптер БЛВС. Драйвер для сетевой интерфейсной карты [network interface card (NIC)] БЛВС – это интерфейс между радиомодулем 802.11 и операционной системой (OS) устройства клиента. По какой бы то ни было причине, драйвер радиомодуля и OS устройства могут взаимодействовать некорректно. Простое включение/выключение NIC радиомодуля перезапустит драйвер. Всегда исключайте эту потенциальную проблему до исследования чего бы то ни было еще. Кроме того, драйвера первого поколения для радиомодулей и прошивки известны возможными ошибками [bug]. Всегда убеждайтесь, что на всем парке клиентских устройств БЛВС установлены последние доступные драйвера. Еще одно изменение, которое быстро и легко можно сделать, – это перенастроить клиентский конфигурационный профиль. Большинство клиентских программ по подключению к Wi-Fi [supplicants] позволяют пользователю определить конфигурационный профиль БЛВС или параметры соединения. Иногда решение проблемы является настолько простым, как удаление старого профиля и настройка нового профиля.

Как упоминалось ранее, проблемы с безопасностью клиентской стороны обычно происходят из неправильно указанных настроек программы по подключению к Wi-Fi. Это может быть чем-то простым, как ошибочно набранный пароль WPA2-Personal, или чем-то сложным, как проблема с цифровым сертификатом 802.1X/EAP.



### Пример из Реальной Жизни

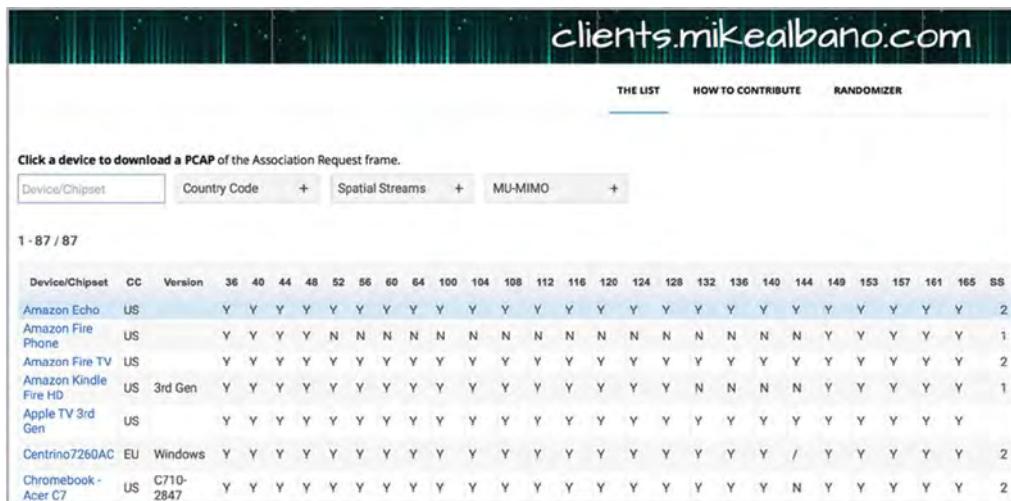
#### Существует ли Главная База Данных Клиентских Wi-Fi Характеристик?

Короткий ответ в том, что не существует официально IEEE базы данных клиентских устройств 802.11 и их характеристик. Однако, существуют несколько ресурсов, включая Wi-Fi Альянс, которые поддерживают базу данных *Поиска СЕРТИФИЦИРОВАННЫХ Wi-Fi Продуктов* [Wi-Fi CERTIFIED Product Finder database] по адресу [www.wi-fi.org/product-finder](http://www.wi-fi.org/product-finder). Хотя большинство производителей инфраструктуры БЛВС отправляют свои точки доступа на сертификацию, нужно понимать, что многие производители клиентских устройств БЛВС не проходят процесс сертификации. Как показано на Рисунке 15.2, Wi-Fi эксперт Майк Альбано [Mike Albano (CWNE #150)] поддерживает свободный публичный список характеристик клиентов БЛВС по адресу [clients.mikealbano.com](http://clients.mikealbano.com). Майк собрал вместе в хорошую базу данных многие современные популярные клиентские устройства БЛВС. На этом онлайн ресурсе вы можете как скачать себе перехваченные кадры 802.11 клиентских устройств, и так и загрузить на сайт информацию о клиенте БЛВС в виде перехваченных пакетов.

Производители ноутбуков или мобильных устройств часто указывают модель радиомодуля в листе спецификации ноутбука или мобильного устройства. Однако, некоторые производители могут не указывать детальную спецификацию радиомодуля и

характеристик. Еще один способ определения радиомодуля Wi-Fi в вашем устройстве – по FCC ID. В Соединенных Штатах, все радиомодули Wi-Fi должны быть сертифицированы государственным агентством - Федеральной Комиссией по Связи [Federal Communications Commission (FCC)]. FCC поддерживает базу данных разрешений на оборудование с возможностью поиска по адресу [www.fcc.gov/fccid](http://www.fcc.gov/fccid). Вы можете ввести FCC ID вашего устройства в поисковую машину базы данных, и найти документацию и фотографии, предоставленные производителем в FCC. База данных FCC очень полезна в помощи определения модели радиомодуля Wi-Fi и спецификации, если информация не доступна на сайте производителя.

**РИСУНОК 15.2** База данных клиентов БЛВС



The screenshot shows a web page titled "clients.mikealbano.com". At the top, there are three tabs: "THE LIST" (which is underlined), "HOW TO CONTRIBUTE", and "RANDOMIZER". Below the tabs, a sub-header reads "Click a device to download a PCAP of the Association Request frame." There are four filter buttons: "Device/Chipset", "Country Code", "Spatial Streams", and "MU-MIMO", each with a plus sign to expand the filter options. The main content is a table with 87 rows, labeled "1 - 87 / 87". The columns represent various wireless parameters: Device/Chipset, CC (Country Code), Version, and then a series of binary values (Y or N) for channel numbers 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144, 148, 153, 157, 161, 165, and SS. The last column contains numerical values representing the count of devices for each row. Some rows include additional information like "3rd Gen" or "Windows".

Device/Chipset	CC	Version	36	40	44	48	52	56	60	64	100	104	108	112	116	120	124	128	132	136	140	144	148	153	157	161	165	SS
Amazon Echo	US		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	2	
Amazon Fire Phone	US		Y	Y	Y	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y	1
Amazon Fire TV	US		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	2	
Amazon Kindle Fire HD	US	3rd Gen	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	1	
Apple TV 3rd Gen	US		Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	
Centrino7260AC	EU	Windows	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	/	Y	Y	Y	2	
Chromebook - Acer C7	US	C710-2847	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	2	

## Надлежащий проект БЛВС уменьшает количество проблем

Две наиболее важные главы для реального мира - это Глава 13 "Концепции Проектирования БЛВС" и Глава 14 "Обследование и Контрольное Обследование". Эти главы являются важными, потому что огромный процент телефонных звонков в поддержку БЛВС является симптомом отсутствия проекта БЛВС. Надлежащее планирование емкости и покрытия, анализ спектра, и контрольное обследование устраниют большую часть обращений в поддержку БЛВС, касающиеся производительности. Надлежащий проект БЛВС заранее минимизирует такие проблемы, как одноканальная интерференция [co-channel interference (CCI)]. Кроме того, многие дыры в безопасности БЛВС могут быть устранены заранее при соответствующем планировании безопасности БЛВС. Если развернуто 802.1X/EAP, то один из наибольших вопросов - это как поместить корневые сертификаты центра сертификации [CA certificates] в мобильные устройства, такие как смартфоны и планшеты. Хорошо продуманная стратегия безопасности для устройств БЛВС сотрудников, устройств BYOD, и гостевого доступа к БЛВС является насущной необходимостью. Надлежащее планирование и проект БЛВС заранее уменьшают время, потраченное на решение проблем БЛВС в дальнейшем.

## БЛВС Всегда Виноват

Несмотря на весь ваш передовой опыт решения проблем БЛВС и лучших усилий, вам стоит смириться с тем фактом, что Wi-Fi всегда будут винить. Опытные администраторы БЛВС знают, что БЛВС будут обвинять в проблемах, которые не имеют ничего общего с Wi-Fi сетью. Это еще одна причина, по которой решение проблем вверх по стеку OSI является важным. Если проблема не является проблемой уровня 1 и уровня 2, то Wi-Fi не виновен. Однако, поставьте себя на место конечного пользователя, который подключен к БЛВС. Технология 802.11 работает на уровне доступа.

Весь смысл ТД - в предоставлении беспроводного портала в уже существующую проводную инфраструктуру. Ваши сотрудники и гости, которые подключены к БЛВС, ожидают бесшовную беспроводную мобильность; у них нет представления о проблемах, которые существуют на уровнях 3-7. Конечный пользователь БЛВС не знает, что DHCP сервер перестал выдавать адреса. Конечного пользователя БЛВС не волнует Провайдер Интернета [Internet service provider (ISP)], который испытывает трудности и то, что канал подключения к оператору (WAN) не работает. Вместо этого, конечные пользователи знают только, что они не могут попасть на [www.facebook.com](http://www.facebook.com) по БЛВС, поэтому они винят Wi-Fi сеть.

## Решение Проблем на Уровне 1

Как ранее обсуждалось, большинство сетевых проблем обычно присутствуют на Физическом уровне. В этом разделе, мы погрузимся глубже в проблемы уровня 1, часто вызванные плохим проектированием БЛВС или радиоинтерференцией. Мы также обсудим проблемы уровня 1, связанные с драйверами радиомодулей, ошибками [bugs] в прошивке, и Питанием по Ethernet [Power over Ethernet (PoE)].

### Проект БЛВС

Ранее вы узнали, что большого объема проблем БЛВС можно избежать при хорошем проекте БЛВС до развертывания. Вероятно, две наиболее распространенные проблемы уровня 1, которые возникают из-за слабого проекта - это дыры в покрытии и одноканальная интерференция. Дыры в покрытии БЛВС обычно являются результатом отсутствия или недостаточности контрольного обследования места. Подтверждение покрытия в  $-70$  дБм для высокоскоростного подключения и  $-65$  дБм для БЛВС голосового качества - строго обязательно. Всегда помните, что приемная чувствительность радиомодулей ТД обычно намного сильнее, чем приемная чувствительность клиентских устройств. Измерения для подтверждения силы принимаемого сигнала должны проводиться с точки зрения клиентских устройств. Из-за широкого разнообразия RSSI клиентских радиомодулей, часто используется клиентское устройство с наименьшей чувствительностью для проверки надлежащей силы сигнала. Более низкая, по сравнению с желаемой силой принимаемого сигнала, приведет к тому что радиомодули переключаться на более низкие скорости передачи данных, которые потребляют больше эфирного времени и негативно влияют на производительность. Вопрос покрытия мертвых зон часто возникает после установки, когда переставлена мебель и даже стены.

Плохое покрытие БЛВС часто является результатом неправильного размещения ТД, а

также неправильной ориентации антенны. Всегда проверяйте техническую спецификацию вашего производителя БЛВС, хотя большинство точек доступа для установки внутри помещений с всенаправленными антеннами с низким усилением должны устанавливаться на потолке, но не выше 3 метров от пола. При использовании внешних всенаправленных антенн, они должны устанавливаться вертикально. Распространенная ошибка - устанавливать их горизонтально. Вы будете шокированы от того, сколько ТД установлены неправильно, часто установлены в надпотолочном пространстве и направлены вверх.

Вы можете посмотреть много фотографий неправильного размещения ТД на <https://badfi.com/bad-fi>, этот забавный блог ведется Эдди Фореро [Eddie Forero, CWNE #160].

Одноканальная интерференция (CCI) является самой частой причиной ненужного потребления эфирного времени, которое можно минимизировать надлежащим передовым опытом проектирования БЛВС. Множественный Доступ с Контролем Несущей и Предотвращением Конфликтов [Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)] описывает полудуплексную связь, когда только один радиомодуль может передавать на одном и том же канале в любое заданное время. Радиомодули 802.11 отложат передачу, если они слышат преамбулу PHY передачи любого другого радиомодуля 802.11 с SNR всего в 4 dB или выше. Ненужная избыточная служебная информация (оверхед) при борьбе за среду, которая происходит, когда слишком много ТД и клиентов слышит друг друга на одном и том же канале, называется *одноканальной интерференцией [co-channel interference (CCI)]*. В действительности, радиомодули 802.11, работают точно так, как определено механизмами CSMA/CA, и это поведение должно в действительности называться как одноканальная совместная работа [co-channel cooperation]. Однако, ненужная избыточная служебная информация при борьбе за среду, вызванная одноканальной интерференцией, обычно является результатом неправильного проекта переиспользования каналов. В то время как почти невозможно предотвратить CCI в полосе 2,4 ГГц, потребление эфирного времени, которое является результатом CCI, может быть минимизировано — и возможно даже устранено — с хорошим передовым опытом проектирования БЛВС в 5 ГГц. Эффективно применяя надлежащую модель переиспользования каналов в 5 ГГц и включая каналы с динамическим выбором частоты [*dynamic frequency selection (DFS)*] уменьшит CCI. Более низкая мощность передачи также уменьшит CCI.

## Мощность Передачи

Еще одна типовая проблема уровня 1 часто бывает, когда устанавливаемые точки доступа настроены на полную мощность по передаче. Хотя у большинства ТД внутри помещений настройки полной мощности передачи могут быть в 100 мВт, они должны редко применяться с полной мощностью. Фактически, это увеличивает фактическую рабочую зону точки доступа; однако, проектирование БЛВС только для покрытия является устаревшей концепцией. Увеличение емкости БЛВС и уменьшение потребления эфирного времени являются более высокими приоритетами. Точки доступа с максимальной мощностью передачи дадут вам избыточное покрытие, но не будут удовлетворять вашим потребностям по емкости. Точки доступа с полной мощностью также увеличат вероятность одноканальной интерференции из-за более проникающей передачи. Далее представлен краткий итог всех проблем, вызванных ТД, передающими на максимальной мощности:

- Потребности по емкости не удовлетворяются
- Увеличение CCI и потреблении эфирного времени, из-за ненужной избыточной служебной информации при борьбе за среду
- Увеличение проблем скрытых узлов
- Увеличение проблем залипших клиентов и проблем с роумингом.

Для всех этих причин, типовая установка БЛВС внутри помещений проектируется с ТД, с установкой мощности от одной четвертой до одной трети от полной мощности передачи. Среды с высокой плотностью пользователей могут требовать, чтобы мощность передачи ТД была установлена в наименьшую настройку - в 1 мВт.

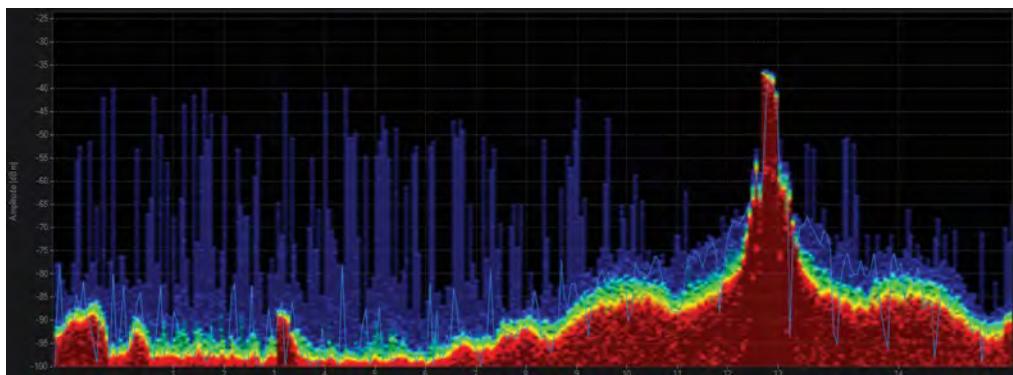
## Радиоинтерференция

Радиоинтерференция от не-802.11 передатчиков безусловно является самой распространенной внешней причиной проблем БЛВС, которые существуют на уровне 1. Пороги обнаружения энергии [*energy detect (ED)*] для не-802.11 передач намного выше, чем пороги обнаружения сигнала [*signal detect (SD)*] для обнаружения радиопередачи 802.11. Однако, различные типы радио интерференции могут все-еще значительно влиять на производительность БЛВС 802.11. Интерферирующие устройства могут превышать порог обнаружения энергии и удерживать радиомодуль 802.11 от передачи, вызывая таким образом отказ в обслуживании [*denial of service*]. Если другой радиоисточник передает с сильной амплитудой, радиомодули 802.11 могут почувствовать радио энергию во время проверки чистоты канала [*clear channel assessment (CCA)*] и отложить передачу целиком. Еще один типовой результат радиоинтерференции в том, что передача кадров 802.11 становится поврежденной. Если кадры повреждены из-за радиоинтерференции, то происходят избыточные повторные передачи, приводящие к значительному уменьшению пропускной способности. Существует несколько разных типов радиоинтерференции, как описано в следующих разделах.

## Узкополосная Интерференция

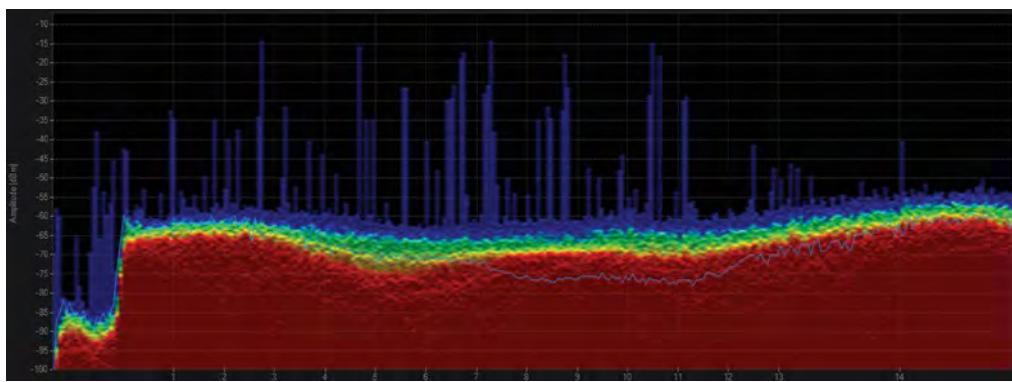
Узкополосный радиосигнал занимает небольшое и ограниченное частотное пространство, и не приводит к отказу в обслуживании [*denial of service (DoS)*] для всей полосы, такой как 2,4 ГГц ISM полоса. Узкополосный сигнал обычно имеет очень высокую амплитуду и полностью разрушает связь в пространстве частот, в котором он передается. Узкополосные сигналы могут разрушить один или несколько каналов 802.11.

Узкополосная радиоинтерференция может также привести к повреждению кадров и повторным передачам на уровне 2. Единственный способ устраниТЬ узкополосную интерференцию – это локализовать интерферирующее устройство-источник с помощью анализатора спектра и убрать интерферирующее устройство. Для работы рядом с помехой используйте анализатор спектра, чтобы определить пострадавшие каналы и затем спроектировать план переиспользования каналов вокруг интерферирующего узкополосного сигнала. Рисунок 15.3 показывает картину анализатора спектра узкополосного сигнала близкого к 11 каналу в полосе 2,4 ГГц ISM.

**РИСУНОК 15.3** Узкополосная радиоинтерференция

### Широкополосная Интерференция

Источник интерференции обычно считается широкополосным, если передаваемый сигнал может повредить связь целой полосы частот. Существуют станции широкополосного подавления, которые могут создать полный DoS для полосы ISM 2,4 ГГц. Единственный способ устраниТЬ широкополосную интерференцию – это найти источник интерферирующего устройства анализатором спектра и убрать интерферирующее устройство. Рисунок 15.4 показывает монитор анализатора спектра с широкополосным сигналом в полосе ISM 2,4 ГГц со средней амплитудой в -70 дБм, которая намного выше определенного порога обнаружения энергии радиомодулей 802.11.

**РИСУНОК 15.4** Широкополосная Радиоинтерференция

### Всеполосная Интерференция

Термин *всеполосная интерференция* [*all-band interference*] обычно связан со связью на основе расширения спектра со скачкообразным перестроением частоты [frequency-hopping spread spectrum (FHSS)], которая обычно разрушает связь 802.11 в 2,4 ГГц. Как вы узнали из ранних глав, FHSS постоянно прыгает по всей полосе, скачкообразно передавая на очень малых поднесущих частотного пространства. Устаревший радиомодуль 802.11 FHSS, например, передает на небольших несущих частотах (*hops*), которые имеют 1 МГц в ширину в полосе 2,4 ГГц. Радиомодули 802.11b передают стационарно в частотном

пространстве 22 МГц, а радиомодули 802.11g/n/ax передают на фиксированных каналах в 20 МГц спектра. Перестраиваясь и передавая, FHSS будет передавать в областях пространства частот, занимаемого фиксированным каналом 802.11.

Хотя устройство FHSS обычно не вызывает отказ в обслуживании [denial of service], передачи кадров от существующих WI-Fi радиомодулей 2,4 ГГц могут быть повреждены всеполосными передачами устаревшего интерферирующего радиомодуля 802.11 FHSS.

Хорошая новость в том, что технологии 802.11 FHSS 20 лет, и она редко встречается развернутой на предприятии. Однако, много других типов радиомодулей со скачкообразным перестроением частоты могут вызвать всеполосную интерференцию.



## Пример из Реальной Жизни

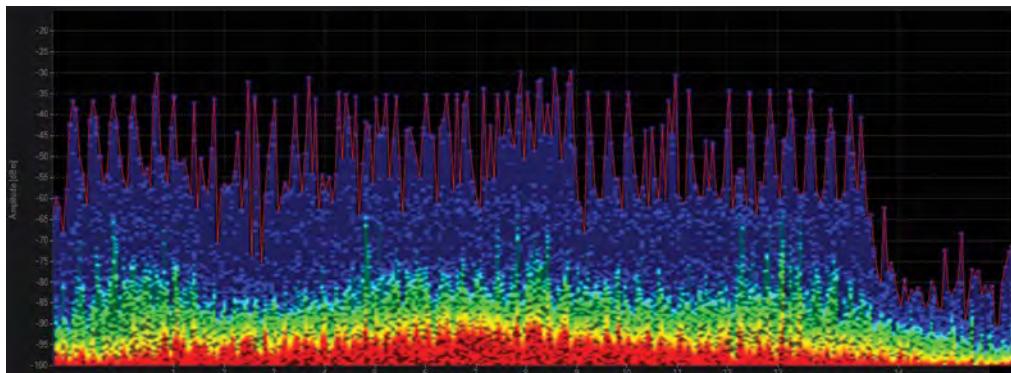
### Какие Устройства Вызывают Радио Интерференцию?

Многочисленные устройства—включая беспроводные телефоны, микроволновые печи, и видеокамеры—могут вызвать радиоинтерференцию и ухудшить производительность БЛВС 802.11. Полоса ISM 2,4 ГГц чрезвычайно переполнена многими известными интерферирующими устройствами. Интерферирующие устройства также передают в полосах U-NII 5 ГГц, но частотное пространство 2,4 ГГц переполнено намного больше. Инструмент, который необходим для локализации источника радиоинтерференции – это анализатор спектра. К счастью, большинство БЛВС предприятий требует использование полосы 5 ГГц, которая менее заполнена и имеет больше частотного пространства. Однако, 5 ГГц радиоинтерференция также существует, поэтому мониторинг анализа спектра необходим.

*Bluetooth (BT)* - это радиотехнология для коротких дистанций, используемая в WPANs. Bluetooth использует FHSS и перестроение частот по полосе ISM 2,4ГГц с частотой 1600 перестроений (скачков) в секунду. Старые устройства Bluetooth были известной причиной жесткой всеполосной интерференции. Более новые устройства Bluetooth используют адаптивные механизмы, чтобы избежать интерференции с БЛВС 802.11. Адаптивное частотное перестроение Bluetooth наиболее эффективно по предотвращению интерференции с одной ТД, передающей на одном канале 2,4 ГГц. Если несколько 2,4 ГГц ТД передают на каналах 1, 6 и 11 на одной и той же территории, передатчикам Bluetooth невозможно избежать интерференции с БЛВС. Беспроводные телефоны стандарта DECT [Digital Enhanced Cordless Telecommunications (DECT)] также используют передачу с перестройкой частоты. Ныне выведенная из эксплуатации технология БЛВС с названием HomeRF [Домашнее Радио] также использовало FHSS; следовательно, устройства HomeRF могли потенциально вызвать всеполосную интерференцию. Другие устройства с перестроением частоты, с которыми вы можете пересечься, включают различные типы устройства медицинской телеметрии. Хотя все интерферирующие источники FHSS, упомянутые до настоящего времени, передают в полосе ISM 2.4 ГГц, 5 ГГц передатчики с перестройкой частоты, которые могут вызвать интерференцию, также существуют.

Передатчики с перестроением частоты обычно не приводят к такому большому повреждению данных, как передатчики фиксированных каналов; однако, существование большого числа передатчиков с перестроением частоты в ограниченном пространстве может привести к большому количеству повреждению данных 802.11 и особо разрушительно для VoWiFi связи. Единственный способ устраниТЬ всеполосную интерференцию – найти интерферирующее устройство с помощью анализатора спектра и убрать интерферирующее устройство. Рисунок 15.5 показывает картину анализатора спектра передачи с перестроением частоты в полосе ISM 2.4 ГГц. После обнаружения источников интерференции, лучшее и простое решение – полностью убрать их.

**РИСУНОК 15.5** Всеполосная радиointерференция



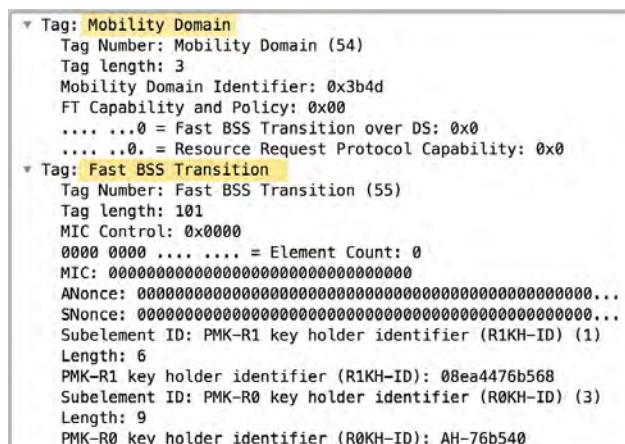
## Драйверы

Как упоминалось ранее, драйверы первого поколения для клиентских устройств часто являются причиной проблем со связью и роумингом. Всегда проверяйте у производителя клиентского устройства, чтобы убедиться, что вы используете последние драйвера.

Еще одна вещь, которую надо помнить, это обратная совместимость между более новыми точками доступа и старыми клиентскими устройствами. Хотя поправки 802.11 обеспечивают обратную совместимость, в реальном мире чаще верно обратное. Устаревшие клиентские драйвера не знают, как обрабатывать новые поля в информационных элементах 802.11, находящихся в маяке и других кадрах управления, передаваемых ТД. Когда на ТД включаются новые технологии, устаревшие клиенты не могут больше подключаться.

Например, проблемы роуминга и подключения могут быть прямым результатом отсутствия поддержки механизмов 802.11k/r/v на клиенте. Рисунок 15.6 изображает два информационных элемента, которые видны в кадрах управления, отправленных ТД с включенным 802.11r. Информационный элемент домена мобильности [*mobility domain information element (MDIE)*] и информационный элемент быстрого перехода BSS [*fast BSS transition information element (FTIE)*] являются полями информации, необходимой для ТД и клиентов, которые поддерживают возможности роуминга Голоса для Предприятий [Voice-Enterprise roaming]. Драйвера устаревших клиентов, которые не поддерживают 802.11r, могут игнорировать эти информационные поля, и все будет хорошо. Но устаревшие клиентские драйвера могут также быть сбиты с толку информационными элементами 802.11r, и могут произойти проблемы с клиентским подключением.

**РИСУНОК 15.6** Информационный элемент быстрого перехода BSS [Fast BSS transition]



Большинство предприятий и корпораций могут устранить многие проблемы клиентского подключения и производительности просто обновив клиентские устройства, принадлежащие компании, до обновления инфраструктуры БЛВС. К сожалению, обычно наиболее часто происходит обратное, компании тратят сотни тысяч долларов на обновление технологий путем покупки новых точек доступа, при этом не меняя устаревших клиентов.

## PoE

В Главе 12 “Питание по Ethernet (PoE)”, мы обсудили важность правильного планирования бюджета мощности PoE. Производители БЛВС обычно получают звонки на поддержку от заказчиков, жалующихся, что все точки доступа внезапно случайным образом начали перегружаться. В большинстве случаев, корневая причина перегрузки ТД случайным образом в том, что бюджет мощности коммутатора превышен. Очень часто, если ТД не может получить мощность, которая ей требуется, то она будет перегружаться и пытаться снова. Бюджет по мощности коммутатора или нескольких коммутаторов должен контролироваться, чтобы гарантировать, что все устройства могут получить питание. Информацию об активном бюджете мощности обычно можно посмотреть из командной строки коммутатора или из графического (GUI) интерфейса, или мониторинга центральной системы управления сети [network management system (NMS)].

Хотя надлежащее планирование бюджета мощности может предотвратить эту проблему во время фазы проектирования, помните, что другие устройства, такие как настольный VoIP телефон, также используют PoE. Дополнительные устройства с питанием PoE могут быть включены в коммутатор приводя к перегрузке бюджета мощности. Надлежащее планирование бюджета мощности и его мониторинг для точек доступа и любых других устройств с PoE является первостепенным. Проблемы с бюджетом мощности вырастут с появлением большего количества точек доступа  $4 \times 4:4$ , которые будут требовать больше 15,4 ватта по определению 802.3af. Модернизация до ТД  $4 \times 4:4$  будет требовать, как минимум пересчет бюджета мощности PoE. По мере добавления производителями БЛВС радиотехнических цепей, радиомодулей двух диапазонов и фактически радиомодулей трех диапазонов, управление бюджетом мощности будет еще более значимым при таком развитии.

PoE, предоставляемое коммутатором, может быть вашим другом, когда вы пытаетесь решить проблемы с ТД, которая по какой-либо причине может быть недоступна из удаленного места. Например, ТД может быть нерабочей из-за перегрузки процессора и может больше не мониторится NMS или недоступна по SSH. Простая принудительная перегрузка ТД может восстановить связь. Один из старых трюков, используемый сетевыми администраторами, - *перезапустить питание [power cycle]* порта оборудования подачи питания [*power-sourcing equipment (PSE)*] коммутатора доступа, который подает питание не отвечающей ТД. Выключение [Disabling] и включение [enabling] питания – принудительно перегружает ТД, которая может быть зависшей.

## Ошибки в Прошивке

Как упоминалось ранее, более старые клиентские прошивки (ПО) и драйвера часто являются причиной проблем с подключением с более новыми моделями ТД. Наоборот, обновляя точки доступа на новое программное обеспечение может также привести к неожиданному подключению к БЛВС и, что более часто, проблемам с производительностью. Как и с любым типом сетевых устройств, обновление операционной системы ТД часто нужно, когда производители БЛВС вводят новые функции и возможности. До выпуска нового кода ТД, производители БЛВС проводят *регрессивное тестирование [regression testing]*, которое проверяет, что ранее разработанные характеристики и возможности продолжают работать и выполняться тем же самым способом. Несмотря на регрессивное тестирование, новые ошибки [bugs] производительности могут появиться, когда новое ПО (прошивка) устанавливается в среде предприятия.

Предлагаемый передовой опыт по развертыванию будет таким: обновляете ТД на стенде или в области выделенной под стенд для тестирования перед крупномасштабной установкой. Еще одна стратегия будет такой: обновляете все ТД в одном здании с активными клиентами, и смотрите, появятся ли новые проблемы.

Если подтверждено, что прошивка (ПО) стабильная, то можно проводить полное обновление по всей компании. У крупных предприятий часто есть четко определенные процессы управления изменениями для выполнения любых типов изменений на сети, включая обновление прошивок (ПО). Всегда, когда это возможно должно проводится надлежащее тестирование прежде чем начать использовать новые клиентские устройства в БЛВС предприятия.

При решении проблем с возможными ошибками в ПО [bugs], понадобится привлечь персонал поддержки вашего производителя БЛВС. Вас вероятнее всего попросят предоставить логи технических данных [tech data logs] и возможно перехват пакетов [packet captures]. Многие производители БЛВС могут также предложить старую золотую версию прошивки (ПО), которая была тщательно протестирована в корпоративных средах и считается лучшим выбором в терминах гарантии качества. Нужно понимать, что более старые версии ТД или контроллера БЛВС могут не иметь новых функций, которые бы вы хотели. Еще одно преимущество обновления ТД на более новое ПО в том, что ранее обнаруженные ошибки в ПО [bugs] могут быть исправлены в новых выпусках ПО.

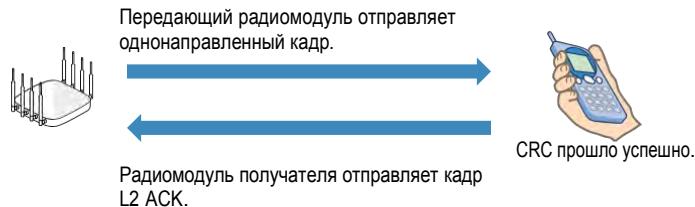
Если обнаружена новая ошибка [bug] в ПО при обновлении ТД, команда поддержки производителя БЛВС может порекомендовать вам откатить обратно ПО вашей ТД на предыдущую версию пока ошибка не будет обработана. При обновлении любых точек доступа, контроллеров БЛВС, или других сетевых устройств, всегда читайте замечания к выпуску [release notes], чтобы узнать о новых функциях, исправленных ошибках, и известных проблемах.

## Решение проблем на Уровне 2

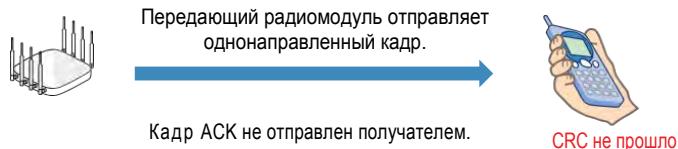
Радиомодули Wi-Fi взаимодействуют путем обмена кадрами 802.11 на МАС подуровне Канального уровня [Data- Link layer]. Следовательно, следующий логический уровень для решения проблем в модели OSI это уровень 2. Этот раздел охватывает многие причины повторных передач на уровне 2 и значительные негативные эффекты, которые они вызывают. При решении проблем БЛВС вы всегда должны мониторить параметры повторных передач уровня 2.

### Повторные передачи Уровня 2

Смертельный враг производительности БЛВС - это повторные передачи уровня 2, которые происходят на МАС подуровне. Как показано на Рисунке 15.7, все односторонние [unicast] кадры 802.11 должны быть подтверждены. В конце каждого кадра есть *циклическая резервная проверка* [cyclic redundancy check (CRC)]. Радиомодуль получателя 802.11 использует CRC кадра, чтобы подтвердить целостность данных полезной нагрузки входящего кадра. Если CRC прошло успешно, то значит кадр не был поврежден во время передачи. Радиомодуль получателя 802.11 тогда отправляет кадр подтверждения 802.11 [802.11 acknowledgment (ACK) frame] обратно исходному передатчику. Кадры ACK Уровня 2 используются в качестве метода подтверждения доставки.

**РИСУНОК 15.7** Подтверждение [ACK] Уровня 2

Если произошла коллизия или любая часть одностороннего [unicast] кадра повреждена, то CRC не пройдет, и принимающий радиомодуль 802.11 не вернет кадр ACK передающему радиомодулю 802.11. Как показано на Рисунке 15.8, если кадр ACK не получен исходным передающим радиомодулем, то односторонний кадр неподтвержден, и должен быть отправлен повторно. Кроме того, агрегированные кадры A-MPDU подтверждаются Блоковым ACK; если один из агрегированных кадров поврежден, то только поврежденный кадр должен быть отправлен повторно, а не весь A-MPDU. Однако, любые кадры, которые должны быть отправлены повторно, создают дополнительную служебную информацию MAC уровня [overhead] и потребляют больше эфирного времени в полудуплексной среде.

**РИСУНОК 15.8** Повторная передача Уровня 2

Передающий радиомодуль осуществляет повторную L2 передачу.

Чрезмерные повторные передачи на 2ом уровне пагубно влияют на БЛВС двумя путями. Первый, повторные передачи на 2 уровне увеличивают потребляющую эфирное время служебную информацию (оверхед), и, следовательно, уменьшают пропускную способность. Хотя другие факторы тоже могут влиять на пропускную способность, но обычно причиной являются обильные повторные передачи на 2 уровне.

Второй, если данные приложений повторно передаются на уровне 2, доставка трафика приложений начинает идти с задержкой или непоследовательно. Приложения, такие как VoIP, зависят от своевременной и упорядоченной доставки IP пакетов. Избыточные повторные передачи 2 уровня обычно приводят к проблемам с задержкой и джиттером для чувствительных ко времени приложений, таких как голос и видео. При обсуждении VoIP, люди часто запутываются касательно разницы между задержкой и джиттером.

**Задержка [Latency]** *Задержка* - это время, занимаемое при доставке пакета от устройства-источника к устройству-назначению. В идеале, задержка не должна превышать 50 миллисекунд для VoIP пакета. Задержка в доставке (увеличенная задержка) VoIP пакета из-за повторных передач уровня 2 может привести к проблемам с эхо.

**Джиттер [Jitter]** *Джиттер* - это вариация задержки. Джиттер измеряет на сколько задержка каждого пакета отличается от средней. Если все пакеты проходят через сеть с одной и той же скоростью, то джиттер будет ноль. Большая вариация задержки (джиттер) является типовым результатом повторных передач на 2 уровне 802.11.

Джиттер приводит к прерывистой голосовой связи, а постоянные повторные передачи приведут к уменьшению срока жизни батареи для VoWiFi телефонов. Хотя клиентские устройства используют буферы для джиттера, чтобы компенсировать вариацию задержки, они обычно эффективны только для вариации задержек меньше 100 миллисекунд. Буферы для джиттера не компенсируют высокий процент повторных передач уровня 2. Вариация джиттера меньше 5 миллисекунд - это идеальная цель для VoWiFi.

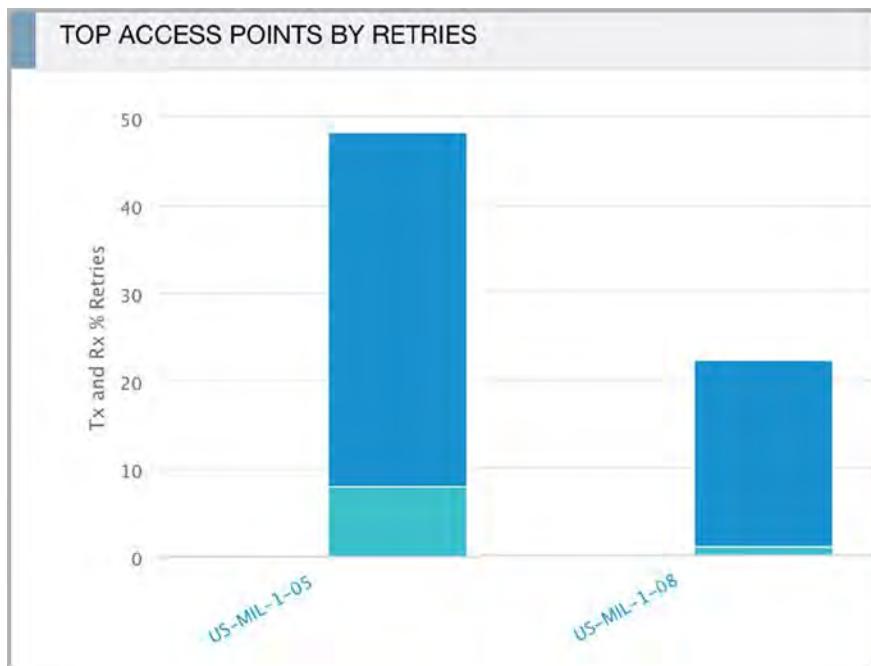
Большинство приложений по передаче данных в Wi-Fi сетях могут справляться с коэффициентом повторных передач на 2 уровне до 10 процентов без какого-либо заметного ухудшения в производительности. Однако, чувствительные ко времени приложения, такие как VoIP, требуют, чтобы потери более высокого уровня IP пакетов были не более 2 процентов. Следовательно, для Голосовых сетей поверх Wi-Fi [Voice over Wi-Fi (VoWiFi)] нужно ограничить повторные передачи 2 уровня до 5 процентов или меньше, чтобы обеспечить своевременную и упорядоченную доставку VoIP пакетов. VoWiFi связь обычно ограничена 5 ГГц, потому что поддерживать коэффициент повторов в 5 процентов на 2м уровне в переполненной полосе 2,4 ГГц редко удается.

Как можно измерить количество повторных передач уровня 2? Любой хороший анализатор протокола 802.11 может отслеживать статистику повторов уровня 2 для всей БЛВС. Анализаторы протоколов 802.11 также могут отслеживать статистику повторов каждой отдельной точки доступа БЛВС и клиентской станции. Как показано на Рисунке 15.9, статистика повторов уровня 2 обычно мониторится централизованно с использованием ТД по всей БЛВС предприятия из контроллера БЛВС или из системы управления сетью [network management system (NMS)]. Так как статистика повторов представляется с точки зрения радиомодулей ТД, то статистика по передаче [transmit (TX)] показывает замеры повторных передач в нисходящем канале связи [downlink] от

**692** Глава 15 • Решение Проблем БЛВС

радиомодуля ТД, в то время как статистика по приему [receive (RX)] показывает замеры клиентских повторных передач в восходящем канале связи [uplink]. Даже чистая радиосреда будет всегда иметь некоторые повторные передачи уровня 2. Цель должна быть 10 процентов или меньше, и 5 процентов или меньше для БЛВС с поддержкой голоса. Превышение коэффициента повторов в 20 процентов почти всегда наносит удар по производительности.

**РИСУНОК 15.9** Статистика повторных передач Уровня 2.



К сожалению, повторные передачи уровня 2 являются результатом многих возможных проблем. Многолучевое распространение [multipath], радиоинтерференция, и низкое отношение сигнал-шум (SNR) являются проблемами, которые существуют на уровне 1, но приводят к повторным передачам на уровне 2. Другие причины повторных передач уровня 2 включают в себя: скрытые узлы, несовпадающие настройки мощности, и интерференцию смежных каналов, которые обычно являются симптомами ненадлежащего проектирования БЛВС.

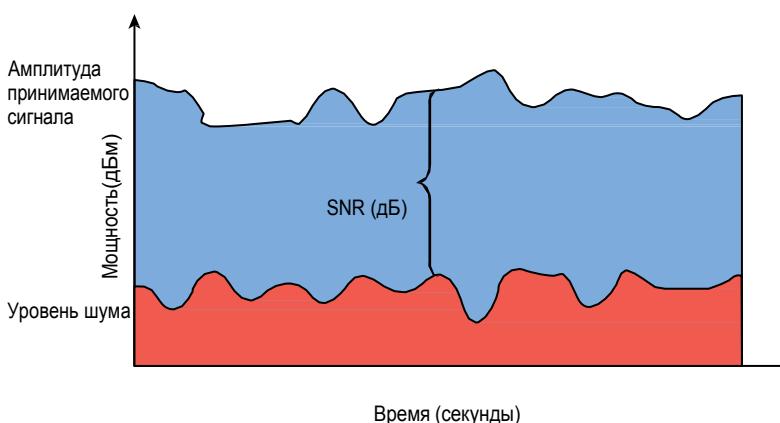
## Радиоинтерференция

Радиоинтерференция от не-802.11 передатчиков – номер один среди причин повторных передач уровня 2. Если кадры повреждены из-за радиоинтерференции, то происходят чрезмерные повторные передачи, и, следовательно, значительно уменьшается пропускная способность. Если повторные передачи уровня 2 достигают чрезмерных уровней время от времени или в разное время дня, то виновником скорее всего является некоторого рода интерферирующее устройство, такое как микроволновая печь. Хороший анализатор спектра БЛВС использует файл радио сигнатур, чтобы помочь вам идентифицировать источник радиоинтерференции. Чтобы остановить повторные передачи на 2м уровне, найдите с помощью анализатора спектра интерферирующее устройство и уберите интерферирующее устройство.

## Низкое SNR

Вероятно, номер два из распространенных причин повторных передач уровня 2 – это низкое соотношение сигнал-шум (SNR). *Отношение сигнал-шум [signal-to-noise ratio (SNR)]* является важным значением, потому что если фоновый шум находится близко к принимаемому сигналу или уровень принимаемого сигнала слишком низок, то данные могут быть повреждены и повторные передачи уровня 2 возрастут. SNR в действительности не совсем отношение. Это просто разница в децибелах между принятым сигналом и фоновым шумом (уровнем шума), как показано на Рисунке 15.10. Если радиомодуль 802.11 принимает сигнал  $-70$  дБм, а уровень шума измеряется в  $-95$  дБм, разница между принятым сигналом и фоновым шумом составляет 25 дБ. Следовательно, SNR равен 25 дБ.

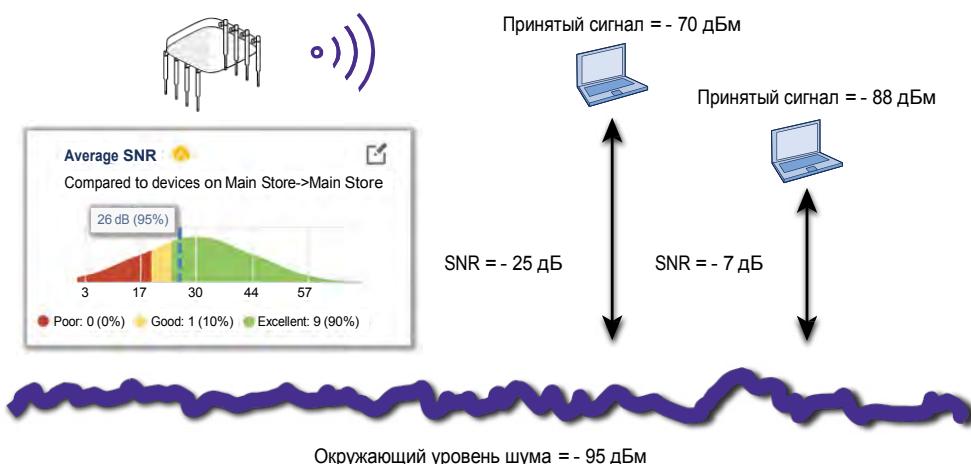
**РИСУНОК 15.10** Отношение сигнал-шум



Передача данных может стать поврежденной при очень низком SNR. Если амплитуда уровня шума слишком близка к амплитуде принятого сигнала, то произойдет повреждение данных и это приведет к повторным передачам уровня 2. Считается, что SNR в 25 дБ или больше - это хорошее качество сигнала, а SNR 10 дБ или меньше, считается, плохим качеством сигнала. Чтобы гарантировать, что кадры были не поврежденными, многие производители рекомендуют минимальный SNR в 20 дБ для БЛВС с передачей данных, и минимальный SNR в 25 дБ для БЛВС с передачей голоса. SNR меньше 20 дБ приведет к переключению ТД и клиентских станций на меньшую модуляцию и схему кодирования [*modulation and coding scheme (MCS)*] и меньшие скорости передачи данных. Более низкие скорости передачи данных потребляют больше эфирного времени и понижают производительность. Кроме того, SNR в 10 дБ или ниже почти всегда гарантирует более высокий процент повторов на уровне 2 из-за повреждения данных, а, следовательно, и слабую производительность.

Как вы узнали из Главы 13, когда вы проектируете покрытие, обычный рекомендуемый передовой опыт - это обеспечить принимаемый сигнал в -70 дБм или сильнее, что обычно намного выше уровня шума. Это гарантирует высокий SNR. При проектировании БЛВС для клиентов VoWiFi, рекомендуется -65 дБм или более сильный сигнал, что еще выше над уровнем шума. Рисунок 15.11 показывает уровень шума в -95 дБм. Когда клиентская станция принимает сигнал -70 дБм от точки доступа, SNR равен 25 дБ; следовательно, в результате нет поврежденных данных. Однако, другой клиент принимает более слабый сигнал в -88 дБм и очень низкий SNR в 7 дБм. Из-за того, что принятый сигнал слишком близок к уровню шума, то произойдет повреждение данных, и как результат повторные передачи уровня 2.

**РИСУНОК 15.11** Высокое и низкое отношения сигнал-шум

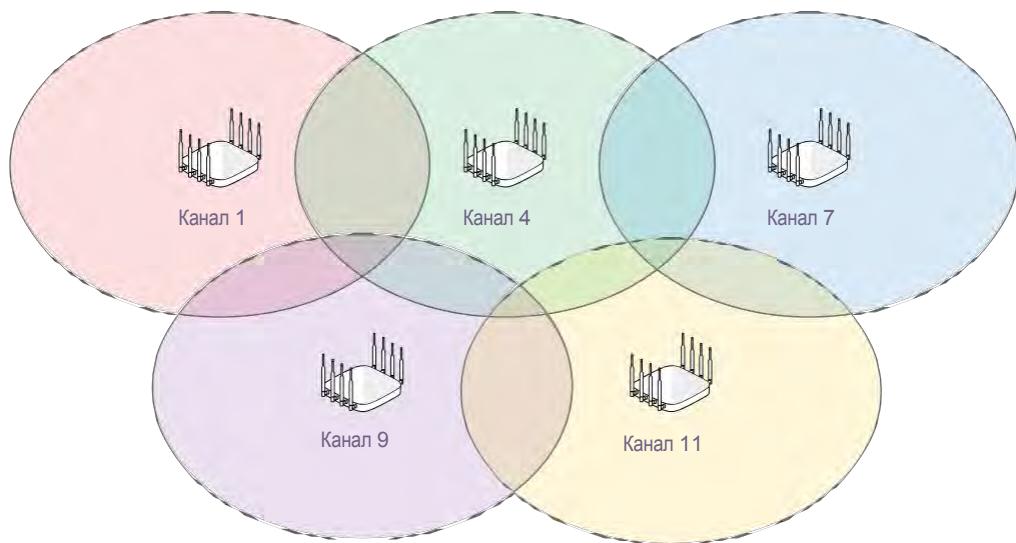


## Интерференция Смежных Каналов

Большинство производителей Wi-Fi используют термин *интерференция смежных каналов* [*adjacent channel interference*], чтобы указать на деградацию производительности в результате перекрывания частотных пространств, которое происходит из-за ненадлежащего дизайна переиспользования каналов. В отрасли БЛВС, смежным каналом считается

следующий или предыдущий по номеру канал. Например, канал 3 является смежным каналом к каналу 2. Рисунок 15.12 изображает перекрывающиеся покрытие зон (сот), которые также перекрываются и по частотному пространству, это приводит к повреждению данных и повторным передачам уровня 2. Каналы 1 и 4, каналы 4 и 7, и каналы 7 и 11 все имеют пересечение по частотному пространству в полосе 2,4 ГГц. Интерференция смежных каналов может вызвать задержку передач 802.11 и повреждение данных, что ведет к повторам на уровне 2. Проблемы производительности, которые являются результатом интерференции смежных каналов, обычно происходят из-за слабого планирования БЛВС в 2,4 ГГц. Использование в 2,4 ГГц модели переиспользования каналов 1,6 и 11 является стандартной практикой проектирования БЛВС, которая предотвращает интерференцию смежных зон(сот).

**РИСУНОК 15.1.2** Интерференция смежных каналов



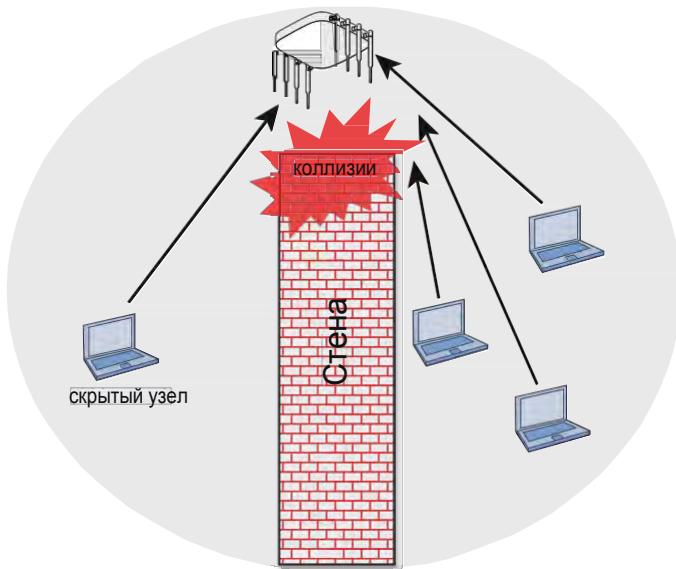
## Скрытый Узел

В Главе 8 "802.11 Доступ к Среде" вы узнали о физическом обнаружении несущей и оценке чистоты канала [clear channel assessment (CCA)]. CCA включает в себя прослушивание радиопередач 802.11 на Физическом уровне; среда должна быть чистой прежде, чем станция сможет передавать. Проблема с физическим обнаружением несущей в том, что не все станции могут слышать друг друга. Помните, что среда является полудуплексной, и в любое выбранное время, только один радиомодуль может передавать. Что же случится, однако, если одна станция, которая хочет передать, проводит CCA, но не слышит другую станцию, которая уже передает? Если станция, которая собирается передавать, не обнаружила никакой радиочастотной энергии во время процесса CCA, она начнет передавать. Проблема в том, что тогда у вас есть две станции, передающие в одно и то же время. Конечный результат - коллизия (столкновение), и кадры станут поврежденными и должны будут отправлены повторно.

Проблема *скрытого узла* [*hidden node*] происходит, когда передачи одной клиентской станции слышны точке доступа, но не слышны другой или всем остальным клиентским станциям в базовом составе сервиса [basic service set (BSS)]. Клиенты не будут слышать друг друга, и, следовательно, могут передавать в одно и то же время. Хотя точка доступа будет слышать обе передачи, а из-за того, что две клиентские станции передают в одно и то же время на одной и той же частоте, входящая клиентская передача будет повреждена.

Рисунок 15.13 показывает область покрытия точки доступа. Заметьте, что толстая кирпичная стена расположена между одной клиентской станцией и всеми другими клиентскими станциями, которые подключены к точке доступа. Радио передачи единственной станции с одной стороны стены не могут быть услышаны всеми другими клиентскими станциями 802.11, хотя все станции могут слышать ТД. Эта неслышимая станция и есть скрытый узел [*hidden node*]. Что продолжает происходить, так это то, что каждый раз, когда передает скрытый узел, другая станция также передает, и происходит коллизия. Скрытый узел продолжает поддерживать коллизии с передачами от всех других станций, которые не могут его слышать во время оценки чистоты канала. Коллизии продолжаются на регулярной основе, и таким образом создают повторные передачи уровня 2, в итоге приводя к уменьшению пропускной способности. Скрытый узел может увеличить коэффициент повторных передач на 15-20 процентов или еще выше. Повторные передачи, конечно, повлияют на пропускную способность и задержку.

**РИСУНОК 15.13** Скрытый узел—препятствие



Проблема скрытого узла может существовать по нескольким причинам—например, плохой проект БЛВС или препятствие, такое как новая возведенная стена или новый установленный книжный шкаф. Пользователь, передвигающийся за каким-либо препятствием может вызвать проблему скрытого узла. Смартфоны и другие мобильные Wi-Fi устройства становятся скрытыми узлами, потому что пользователи берут свои мобильные устройства в тихие уголки или области, где радиосигнал телефона не может быть слышен другими клиентскими станциями.

Пользователи с беспроводными настольными устройствами часто кладут свои устройства под металлическую столешницу и фактически превращают радиомодуль настольного устройства в неслышимый скрытый узел.

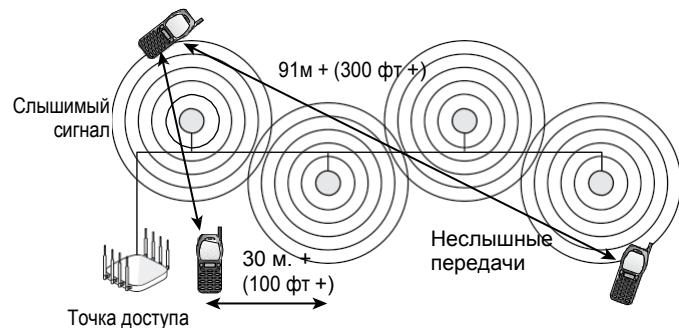
Проблема скрытого узла также может произойти, когда две клиентские станции расположены в противоположных концах зоны (сотовой) радиопокрытия и не могут слышать друг друга, как показано на Рисунке 15.14. Это часто случается, когда фактическое покрытие зоны (сотовой) слишком большое, что является результатом вещания радиомодуля точки доступа с чрезмерным уровнем мощности.

**РИСУНОК 15.14** Скрытый узел—большая зона(сотовая) покрытия



Еще одной причиной проблемы скрытого узла являются распределенные антенные системы. Некоторые производители проектируют распределенные системы, которые в основном сделаны из длинных коаксиальных кабелей с несколькими антенными элементами. Каждая антenna в распределенной системе имеет свою собственную область покрытия. Многие компании покупают распределенную antennную систему [*distributed antenna system (DAS)*] в целях экономии. Распределенные antennные системы и излучающие кабельные системы [*leaky cable systems*] являются специализированными решениями, которые иногда устанавливаются из-за того, что они могут также обеспечить покрытие для частот сотовой телефонии. Проблема скрытого узла, как показано на Рисунке 15.15, почти всегда происходит, если только одна точка доступа подключена к DAS. Если устанавливается решение DAS, то также нужны несколько ТД.

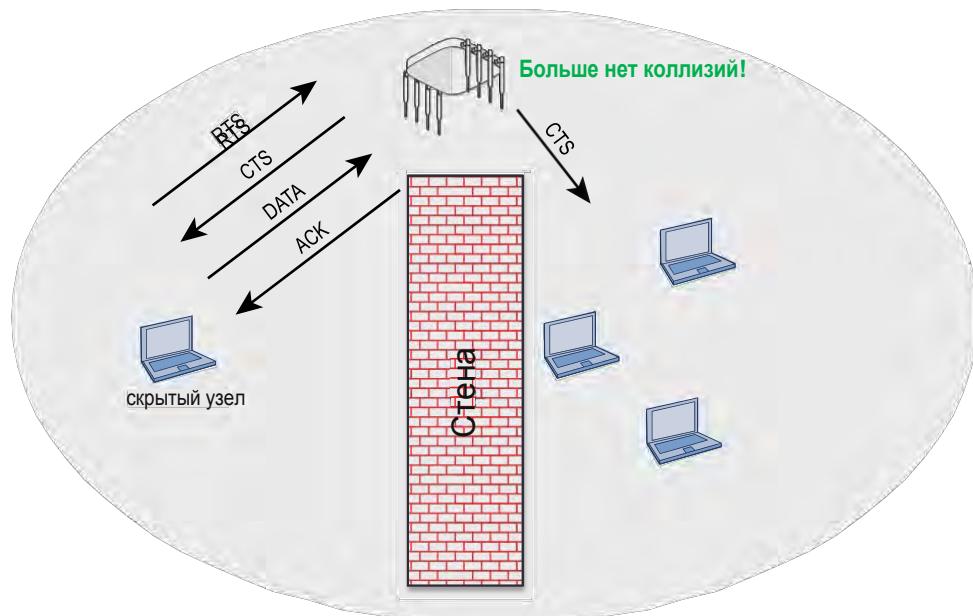
**РИСУНОК 15.15** Скрытый узел—распределенная antennная система



Итак, как вам решать проблему скрытого узла? Если ваши конечные пользователи жалуются на деградацию пропускной способности, то одна из возможных причин - это скрытый узел. Анализатор протоколов является полезным инструментом для определения проблем связанных со скрытым узлом. Если анализатор протоколов показывает более высокий параметр повторных передач для MAC адреса одной станции по сравнению с другими клиентскими станциями, то скрытый узел найден. У некоторых анализаторов протоколов даже есть предупреждения о скрытом узле на основе порогов повторных передач.

Еще один способ - это использование метода запрос-на-отправку/готов-к-отправке [request-to-send/clear-to-send (RTS/CTS)] для диагностики проблемы. Если на клиентском устройстве может быть настроено RTS/CTS, попытайтесь уменьшить порог RTS/CTS на предполагаемом скрытом узле до примерно 500 байт. Например, скажем, вы установили приложение эмуляции терминала в складской среде, и существует проблема скрытого узла. В этом случае, порог RTS/CTS должен быть установлен в максимально малый размер, например, 50 байт. Используйте анализатор протокола, чтобы определить соответствующий размер. Как вы узнали из Главы 9 "802.11 MAC" RTS/CTS - это метод, в котором клиентские станции могут зарезервировать среду для себя. Рисунок 15.16 показывает скрытый узел, инициирующий RTS/CTS обмен.

**РИСУНОК 15.16** Скрытый узел и RTS/CTS



Станции с другой стороны препятствия могут не слышать кадр RTS от скрытого узла, но они услышат кадр CTS, отправленный точкой доступа. Станции, которые слышат кадр CTS переустановят свои NAV на период времени, необходимый для того, чтобы скрытый узел передал кадр данных и получил кадр ACK.

Применение RTS/CTS на скрытом узле резервирует среду и форсирует все станции встать на паузу; таким образом коллизии и повторные передачи уменьшатся.

Коллизии и повторные передачи в результате скрытого узла станут причиной уменьшения пропускной способности. RTS/CTS обычно тоже уменьшает пропускную способность. Однако, если RTS/CTS применен на предполагаемом скрытом узле, то пропускная способность вероятно вырастет из-за остановки коллизий и повторных передач. Если вы применили RTS/CTS на предполагаемом скрытом узле, и пропускная способность увеличилась, то вы подтвердили существование скрытого узла.

Многие устаревшие клиентские устройства 802.11 имели возможность настраивать пороги RTS/CTS. В действительности, на большинстве текущих клиентских устройств не может быть вручную настроены RTS/CTS. Следовательно, RTS/CTS в качестве диагностического инструмента с клиентской стороны обычно - не вариант. Стоит отметить, что из-за того, что проблема скрытого узла происходит часто, радиомодули БЛВС могут автоматически использовать RTS/CTS, чтобы уменьшить проблемы скрытого узла. Автоматическое использование RTS/CTS, скорее всего, будет осуществляться с радиомодулей точки доступа, а не с радиомодулей на стороне клиента.

Пороги RTS/CTS могут всегда быть настроены вручную на точках доступа. Типовое использование ручной настройки RTS/CTS - это мосты точка-многоточка [*point-to-multipoint (PtMP)*]. Некорневые мосты в сценарии PtMP будут не способны слышать друг друга, потому что они могут быть в километрах друг от друга. RTS/CTS должен применяться на некорневых мостах PtMP для устранения коллизий, вызванных мостами - скрытыми узлами, которые не могут слышать друг друга.

Следующие методы могут быть использованы для решения проблемы скрытого узла:

**Использование RTS/CTS.** Используйте или анализатор протоколов, или RTS/CTS для диагностики проблемы скрытого узла. RTS/CTS также может быть использован для автоматического или ручного решения проблемы скрытого узла.

**Увеличение мощности на всех станциях.** У большинства клиентских станций фиксированная выходная мощность передачи. Однако, если выходная мощность может настраиваться на клиентской стороне, то увеличение мощности передачи клиентской станции увеличит дальность действия каждой станции. Если дальность действия передачи всех станций увеличена, то вероятность, что станции будут слышать друг друга, также увеличится. Обычно это является плохой идеей и не рекомендуемым способом решения, потому что увеличение клиентской мощности может увеличить одноканальную интерференцию.

**Устранение препятствий.** Если определено, что какое-то препятствие мешает клиентским станциям слышать друг друга, простое устранение препятствия решит проблему. Очевидно, что вы не можете убрать стену, но если препятствие — это металлический стол или шкаф для бумаг, то оно может быть перемещено, чтобы решить проблему.

**Перемещение скрытого узла.** Если одна или две станции находятся в области, где они стали неслышны, то простое перемещение их в пределах зоны действия передачи других станций решит проблему.

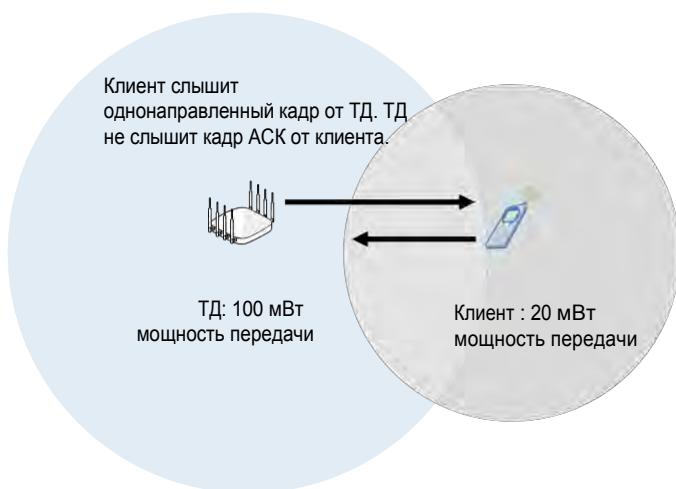
**Добавление еще одной точки доступа.** Если перемещение скрытых узлов не вариант, то добавление еще одной точки доступа в скрытой области для предоставления покрытия исправит проблему. Лучшее решение постоянной проблемы скрытого узла - это добавление еще одной ТД.

## Несовпадающая Мощность

Еще одна потенциальная причина повторных передач на уровне 2 – это несовпадающие настройки мощности передачи между точкой доступа и клиентским радиомодулем. Связь может оборваться, если уровень мощности передачи клиентской станции меньше, чем уровень мощности передачи точки доступа. По мере движения клиента к краю зоны(сотов) покрытия, клиент может “слышать” ТД; однако, ТД не “слышит” клиента. Хорошая новость в том, что эта проблема не происходит часто в средах с высокой плотностью внутри помещений. В последние годы, были существенные улучшения в оборудовании точек доступа. Улучшенная приемная чувствительность радиомодулей ТД фактически решила многие проблемы с несовпадающими настройками мощности клиента и ТД в средах внутри помещений. Проблемы, которые происходят из-за несовпадающих настроек мощности вероятнее всего происходят вне помещений на открытом воздухе.

Как показано на Рисунке 15.17, если у наружной точки доступа мощность передачи 100 мВт, а у клиентской мощность передачи 20 мВт, клиент услышит одн定向енный кадр от ТД, потому что принятый сигнал находится в пределах возможностей приемной чувствительности клиентской станции. Однако, когда клиент посыпает кадр ACK обратно ТД, амплитуда клиентского переданного сигнала падает заметно ниже порога приемной чувствительности радиомодуля ТД. Кадр ACK не “слышен” ТД, которая затем должна повторно отправить одн定向енный кадр. Все клиентские передачи фактически видны как шум для ТД, и в результате получаем повторные передачи на уровне 2.

**РИСУНОК 15.17 Несовпадающая мощность ТД и клиента**



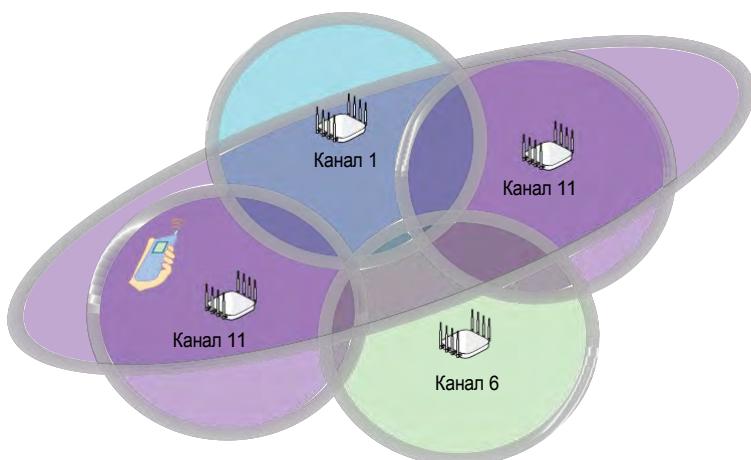
Проблемы мощности ТД/клиент обычно происходят, потому что ТД часто устанавливают на полную мощность, чтобы увеличить дальность действия. Увеличение мощности точки доступа является неправильным путем по увеличению дальности действия. Если вы хотите увеличить дальность действия для клиентов, лучшее решение – это увеличить усиление антенны точки доступа. Многие люди не понимают простого принципа *взаимности антенн* [concept of antenna reciprocity], который подразумевает, что антенны усиливают принятые сигналы также как они усиливают передаваемые сигналы. Антенна с высоким усилением на точке доступа усилит передаваемый ТД сигнал и увеличит дальность действия, при котором клиент сможет слышать сигнал. Антенна ТД с высоким усилением также будет усиливать принятый сигнал от удаленной клиентской станции.

Один из способов проверить есть ли проблема с несовпадающей мощностью ТД/клиент - это послушать анализатором протокола. Проблема с мощностью ТД/клиент есть, если кадры передачи клиентской станции повреждены, при прослушивании эфира около точки доступа, но не повреждены, когда вы слушаете около клиентской станции.

Как вам предотвратить повторы на 2ом уровне, которые вызваны несовпадающими настройками мощности между ТД и клиентами? Лучшее решение - это удостовериться, что все настройки мощности клиентской передачи совпадают с мощностью передачи точки доступа. Однако, значительные улучшения в приемной чувствительности ТД фактически решили многие проблемы несовпадения настроек мощности клиента и ТД. Зная все это, настройка точки доступа на передачу на полной мощности обычно является не очень хорошей идеей, и может вызвать эту проблему, а также и многие другие проблемы, упомянутые ранее в этой главе.

В этом разделе, мы сфокусировались на несовпадающих настройках мощности, которые являются симптомом слишком большой мощности передачи от точки доступа. В реальности, проблема несовпадающей мощности намного больше, когда *клиенты* передают с более высокой мощностью, чем точки доступа внутри помещений. Мощность передачи многих внутренних точек доступа может быть 10мВт или меньше, из-за проектной необходимости по высокой плотности. Однако, большинство клиентов, таких как смартфоны и планшеты, могут передавать на фиксированной амплитуде в 15 мВт или 20 мВт. Так как клиенты часто передают на более высокой мощности, чем ТД, и потому что клиенты мобильны, результатом будет одноканальная интерференция [co-channel interference (CCI)], как показано на Рисунке 15.18. Как ранее упоминалось, CCI приведет к избыточной служебной информации при борьбе за среду (overhead), которая потребляет ценное эфирное время. Чего многие люди не понимают о CCI - это тот факт, что клиенты - это причина номер один одноканальной интерференции (CCI). Вы должны понимать, что CCI не статична и всегда изменяется из-за мобильности клиентских устройств.

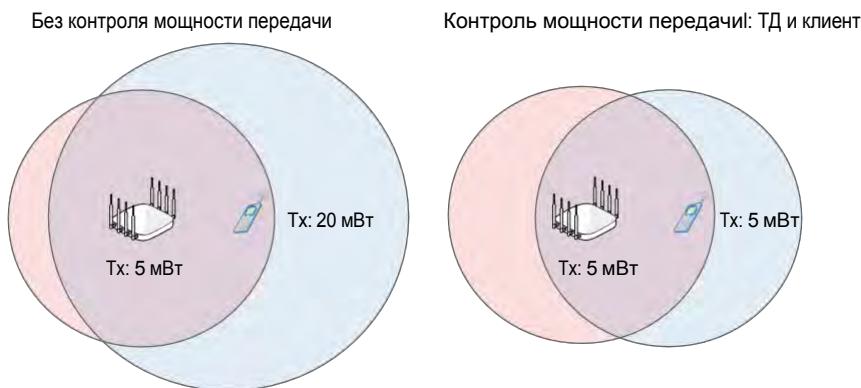
**РИСУНОК 15.18** Одноканальная интерференция на основе клиентов



Точка доступа с включенной возможностью 802.11k может сказать ассоциированным клиентам, чтобы они использовали функции *контроля мощности передачи* [*transmit power control (TPC)*], чтобы изменять свою амплитуду передачи динамически, чтобы соответствовать мощности ТД. Клиенты, которые поддерживают TPC подстроят свою мощность, чтобы соответствовать мощности передаче ТД, как показано на Рисунке 15.19. Применение настроек TPC на ТД значительно уменьшают одноканальную интерференцию, вызванную клиентами. Стоит отметить, однако, что устаревшие клиенты не

поддерживают ТРС, и некоторые устаревшие клиенты могут испытывать проблемы с подключением, если включить ТРС на ТД.

**РИСУНОК 15.19** Контроль мощности передачи



## Многолучевое распространение

Как обсуждалось в Главе 3 "Основы Радиотехники", *многолучевое распространение [multipath]* может вызвать *межсимвольную интерференцию [intersymbol interference (ISI)]*, которая вызовет повреждение данных. Из-за разницы во времени между основным сигналом и отраженными сигналами, называемой *разбросом по времени задержки [delay spread]*, у приемника могут быть проблемы с демодуляцией информации радиосигнала. Разница во времени разброса времени задержки приведет к повреждению данных. Если данные повреждены из-за многолучевого распространения, то в результате будут повторные передачи на уровне 2.

Многолучевое распространение может быть серьезной проблемой при работе с устаревшим оборудованием 802.11a/b/g. Использование направленных антенн часто уменьшает число отражений, и разнесение антенн также можно использовать для компенсации негативных влияний многолучевого распространения. Многолучевое распространение [multipath] - это радиоволновое явление, которое многие годы было причиной деструктивных эффектов, когда применялась старая технология 802.11a/b/g. Однако, так как многие установленные БЛВС обновились до технологий 802.11n или 802.11n/ac, то многолучевое распространение больше не является нашим врагом. Многолучевое распространение теперь имеет конструктивный эффект с передачами 802.11n/ac, которые используют антенны *много-вводов, много выводов [multiple-input, multiple-output (MIMO)]* и методы обработки сигналов *комбинации максимального отношения [maximum ratio combining (MRC)]*.

## Решение Проблем Безопасности

Безопасность 802.11 определяет методы аутентификации на уровне 2 и шифрование на уровне 2. Следовательно, проблемы безопасности БЛВС будут происходить на уровне 2 и приводить к ошибкам в клиентском подключении к БЛВС. Многие производители БЛВС предлагают диагностические инструменты для уровня 2 для решения проблем с аутентификацией и ассоциацией клиентских устройств. Эти инструменты диагностики могут быть доступны прямо из ТД,

контроллера БЛВС, или из облачной системы управления сетью [network management system (NMS)]. Лучшие диагностические инструменты могут даже предложить исправление для обнаруженных проблем. Лог (log) файлы безопасности и AAA с оборудования БЛВС и RADIUS сервера также является великолепным местом для старта при решении проблем с аутентификацией и PSK и 802.1X/EAP. Лог [Log] файлы также могут быть собраны с индивидуальных клиентов БЛВС [WLAN supplicants].

## Решение проблем PSK

Решение проблем аутентификации PSK относительно простое. Инструменты диагностики производителей БЛВС, лог-файлы, или анализатор протоколов, все могут использоваться для наблюдения 4x стороннего процесса рукопожатия [4-Way Handshake process] между клиентом БЛВС и точкой доступа. Давайте сначала взглянем на успешную аутентификацию PSK. На Рисунке 15.20, вы можете увидеть, что клиент ассоциируется с ТД и затем начинается аутентификация PSK. Так как параметры PSK совпадают и на точке доступа и на клиенте, то создается парный мастер ключ [pairwise master key (PMK)] чтобы провести 4x Стороннее Рукопожатие [4-Way Handshake]. Процесс 4x-Стороннего Рукопожатия используется, чтобы создать динамически генерируемые односторонние ключи шифрования, которые уникальны для радиомодуля ТД и радиомодуля клиента.

**РИСУНОК 15.20** Успешная аутентификация PSK

Device Name	Device BSSID	Event Type	Description
12-A-3BD500	08EA443BD514	Basic	Rx assoc req (rss 40dB)
12-A-3BD500	08EA443BD514	Basic	Tx assoc resp <accept> (status 0, pwr 3dBm)
12-A-3BD500	08EA443BD514	Info	WPA-PSK auth is starting (at if=wifi0.1)
12-A-3BD500	08EA443BD514	Info	Sending 1/4 msg of 4-Way Handshake (at if=wifi0.1)
12-A-3BD500	08EA443BD514	Info	Sending 1/4 msg of 4-Way Handshake (at if=wifi0.1)
12-A-3BD500	08EA443BD514	Info	Received 2/4 msg of 4-Way Handshake (at if=wifi0.1)
12-A-3BD500	08EA443BD514	Info	Sending 3/4 msg of 4-Way Handshake (at if=wifi0.1)
12-A-3BD500	08EA443BD514	Info	Received 4/4 msg of 4-Way Handshake (at if=wifi0.1)
12-A-3BD500	08EA443BD514	Info	PTK is set (at if=wifi0.1)
12-A-3BD500	08EA443BD514	Basic	Authentication is successfully finished (at if=wifi0.1)
12-A-3BD500	08EA443BD514	Info	station sent out DHCP DISCOVER message
12-A-3BD500	08EA443BD514	Info	DHCP server sent out DHCP OFFER message to station
12-A-3BD500	08EA443BD514	Info	DHCP server sent out DHCP OFFER message to station
12-A-3BD500	08EA443BD514	Info	station sent out DHCP REQUEST message
12-A-3BD500	08EA443BD514	Info	DHCP server sent out DHCP ACKNOWLEDGE message to station
12-A-3BD500	08EA443BD514	Basic	DHCP session completed for station
12-A-3BD500	08EA443BD514	Basic	IP 10.5.1.162 assigned for station

## 704 Глава 15 • Решение Проблем БЛВС

Рисунок 15.20 показывает, что процесс 4x-Стороннего Рукопожатия был успешен, и что односторонний парный временный ключ [unicast pairwise transient key (PTK)] установлен на ТД и на клиенте. Процесс общения (договоривания) на 2ом уровне завершен, и теперь время для того, чтобы клиент перешел на более высокие уровни. Таким образом, конечно, следующий шаг в том, что клиент получает IP адрес по DHCP. Если клиент не получил IP адрес, то это сетевая проблема, а, следовательно, не проблема Wi-Fi.

Возможно, администратор БЛВС получает телефонный звонок от конечного пользователя, который не может подключиться, используя WPA2-Personal. Большая часть проблем находится на Физическом уровне; следовательно, базовое решение проблем Wi-Fi предписывает, чтобы конечный пользователь сначала выключил и снова включил сетевую Wi-Fi карту. Это должно гарантировать, что драйверы сетевой Wi-Fi карты [Wi-Fi NIC] корректно взаимодействуют с операционной системой. Если проблема с подключением сохранилась, то проблема присутствует на уровне 2. Далее вы можете использовать диагностические инструменты, лог-файлы, или анализатор протоколов, чтобы рассмотреть неудавшуюся аутентификацию PSK клиента БЛВС.

На Рисунке 15.21, вы можете увидеть, что клиент ассоциируется и далее начинает аутентификацию PSK. Однако, процесс 4x Стороннего Рукопожатия не проходит. Обратите внимание, что только два кадра 4x Стороннего рукопожатия завершены.

Проблема почти всегда в несовпадении параметров PSK [PSK credentials]. Если параметры PSK не совпадают, исходный материал парного мастера ключа [pairwise master key (PMK) seed] создается не корректно, и, следовательно, 4x-Стороннее Рукопожатие полностью проваливается. Итоговый парный временный ключ [final pairwise transient key (PTK)] никогда не создается. Существует симбиотическая связь (симбиоз) между аутентификацией и созданием динамических ключей шифрования. Если аутентификация PSK не проходит, то тоже самое делает и 4x-Стороннее Рукопожатие, которое используется для создания динамических ключей шифрования. И нет никакой попытки получить клиентом IP адрес, так как процесс на уровне 2 не завершен.

### РИСУНОК 15.21 Неуспешная аутентификация PSK

2016-02-22 16:06:48	05-A-764fc0	08EA44764FD4	Info	WPA-PSK auth is starting (at if=wifi0.1)
2016-02-22 16:06:48	05-A-764fc0	08EA44764FD4	Info	Sending 1/4 msg of 4-Way Handshake (at if=wifi0.1)
2016-02-22 16:06:49	05-A-764fc0	08EA44764FD4	Info	Received 2/4 msg of 4-Way Handshake (at if=wifi0.1)
2016-02-22 16:06:52	05-A-764fc0	08EA44764FD4	Info	Sending 1/4 msg of 4-Way Handshake (at if=wifi0.1)
2016-02-22 16:06:52	05-A-764fc0	08EA44764FD4	Info	Received 2/4 msg of 4-Way Handshake (at if=wifi0.1)

Когда настроена безопасность PSK, вводится 8-63 знаковый чувствительный к регистру пароль [passphrase] пользователем или администратором. Этот пароль затем используется для создания PSK. Пароль может потенциально быть неправильно настроенным на точке доступа; однако в большинстве случаев, проблема проста: конечный пользователь некорректно набирает пароль. Администратору нужно вежливо попросить конечного пользователя повторно набрать пароль медленно и внимательно, что является хорошим средством от, что называется, *толстых пальцев* [*fat-fingering*].

Еще одна возможная причина неудачи аутентификации PSK может быть в несовпадении выбранных методов шифрования. Точка доступа может быть настроена на поддержку только WPA2 (CCMP-AES), которую устаревшие клиенты WPA (TKIP) не поддерживают. Похожая неудача может произойти и с 4x Сторонним Рукопожатием.

## Решение проблем 802.1X/EAP

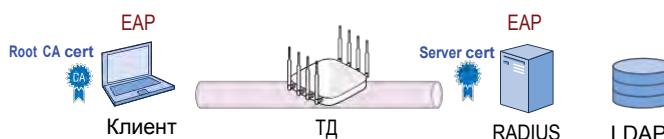
Аутентификация PSK (также называется WPA2-Personal) является простой для решения проблем, потому что метод аутентификации был спроектирован быть несложным. Однако, решение проблем более сложной аутентификации 802.1X/EAP (также называемой WPA2-Enterprise) является большой задачей, потому что существует несколько точек отказа.

802.1X - это стандарт контроля доступа на основе порта, который определяет механизмы необходимые для аутентификации и авторизации устройств к сетевым ресурсам. Структура аутентификации 802.1X состоит из трех главных компонентов, каждый с определенной ролью. Эти три компонента 802.1X работают вместе, чтобы гарантировать, что только подтвержденным надлежащим образом пользователям и устройствам предоставлялся доступ к сетевым ресурсам. Три компонента 802.1X называются: клиент [supplicant] (дословно - проситель), аутентификатор [authenticator], и сервер аутентификации. Клиент [supplicant] – это пользователь или устройство, которое запрашивает доступ к сетевым ресурсам. Работа сервера аутентификации – подтверждать параметры доступа [credentials] клиента [supplicant]. Аутентификатор – это шлюзовое устройство, которое располагается между клиентом [supplicant] и сервером аутентификации, контролирующее или регулирующее доступ клиента к сети.

## Зоны Решения Проблем 802.1X/EAP

На примере, показанном на Рисунке 15.22, клиент [supplicant] – это Wi-Fi клиент, ТД – это аутентификатор, а внешний RADIUS сервер работает как сервер аутентификации. RADIUS сервер может поддерживать внутреннюю базу данных пользователей или запрашивать внешнюю базу данных, например базу данных LDAP. Расширенный Протокол Аутентификации [Extensible Authentication Protocol (EAP)] используется в структуре 802.1X/EAP для подтверждения пользователей на 2ом уровне. Wi-Fi клиенту не будет позволено осуществлять связь на более высоких уровнях 3-7 до тех пор, пока RADIUS сервер не подтвердит идентификацию (личность) клиент [supplicant] на 2ом уровне.

**РИСУНОК 15.22** 802.1X/EAP

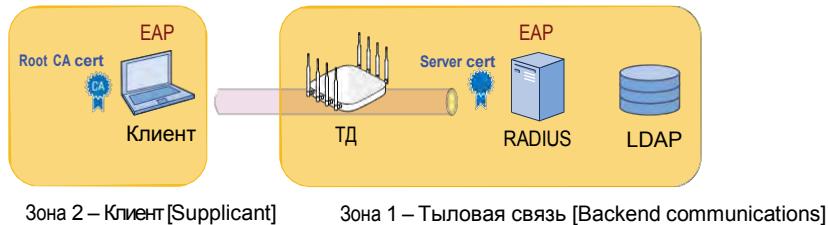


ТД блокирует всю связь более высокого уровня клиента [supplicant] до тех пор, пока клиент [supplicant] не подтвержден. Когда клиент [supplicant] подтвержден, связь на более высоких уровнях разрешена через виртуальный "контролируемый порт" ["controlled port"] на ТД (аутентификаторе). Трафик аутентификации EAP 2ого уровня инкапсулирован в RADIUS пакеты между аутентификатором и сервером аутентификации. Аутентификатор и сервер аутентификации также подтверждают друг друга общим секретом [*shared secret*].

Улучшенные версии EAP, такие как EAP-PEAP и EAP-TTLS, используют туннелированную аутентификацию [*tunneled authentication*], чтобы защитить параметры доступа клиента [supplicant credentials] от автономных атак подбора пароля по словарям [*offline dictionary attacks*]. Сертификаты используются в процессе EAP для создания

шифрованных SSL/TLS туннелей и обеспечения безопасного аутентификационного информационного обмена. Как показано на Рисунке 15.23, серверный сертификат находится на RADIUS-сервере, а корневой публичный сертификат ЦС [root CA public certificate] должен быть установлен на клиенте [supplicant]. Как упоминалось ранее, существует много потенциальных точек отказа в процессе 802.1X/EAP. Однако, как показано на Рисунке 15.23, существует фактически две зоны решения проблем в структуре 802.1X/EAP где происходят отказы [failures]. Зона 1 решения проблем состоит из тыловой связи или связи с серверами [backend communications] между аутентификатором, сервером аутентификации, и базы данных LDAP. Зона 2 решения проблем располагается только на клиентском [supplicant] устройстве, которое запрашивает доступ.

**РИСУНОК 15.23** Зоны решения проблем 802.1X/EAP



## Зона 1: Проблемы Тыловой Связи

Всегда сначала нужно исследовать Зону 1. Если ТД и RADIUS сервер не могут связываться друг с другом, то весь процесс аутентификации не состоится. Если RADIUS-сервер и база данных LDAP не могут взаимодействовать, то весь процесс аутентификации также не состоится.

Рисунок 15.24 представляет запись попыток клиента [supplicant] (Wi-Fi клиента) связаться с RADIUS сервером. Аутентификатор пересыпает запрос RADIUS серверу, но RADIUS сервер не отвечает. ТД (аутентификатор) тогда посыпает кадр деаутентификации Wi-Fi клиенту, потому что процесс не удался. Это является показателем, что существует проблема с тыловой [backend] связью в первой зоне решения проблем.

**РИСУНОК 15.24** RADIUS сервер не отвечает.

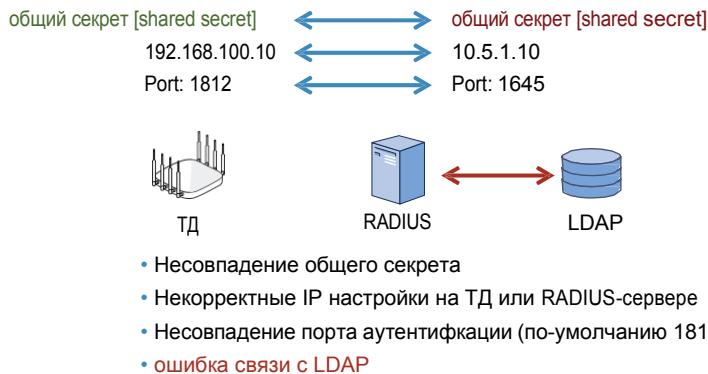
```
Rx assoc req (rssi 91dB)
IEEE802.1X auth is starting (at if=wifi0.1)
Sending EAP Packet to STA: code=1 (EAP-Request) identifier=0 length=5
received EAPOL-Start from STA
Sending EAP Packet to STA: code=1 (EAP-Request) identifier=1 length=5
received EAP packet (code=2 id=1 len=36) from STA: EAP Response-Identity (1),
Send message to RADIUS Server(10.5.1.20): code=1 (Access-Request) identifier=
received EAPOL-Start from STA
Sending EAP Packet to STA: code=1 (EAP-Request) identifier=3 length=5
received EAP packet (code=2 id=3 len=36) from STA: EAP Response-Identity (1),
Send message to RADIUS Server(10.5.1.20): code=1 (Access-Request) identifier=
Sta(at if=wifi0.1) is de-authenticated because of notification of driver
```

AH Device	User	Problem Type	Detected On	Last Successful Connection	Take Action
● 0X-AP		Auto Generated	2016-02-15 21:57:01	2016-02-15 22:58:33	
Location	User Profile				
		Description		Suggested Remedy	
Client MAC		Could not reach the RADIUS server.		Verify that the RADIUS server is up and reachable over the network.	
000E3B3330B8					
Case Number					
Assign					

Как показано на Рисунке 15.25, если RADIUS-сервер не отвечает клиенту [supplicant], то существует четыре возможные точки отказа в первой зоне решения проблем:

- Несовпадение общего секрета (пароля)
- Некорректные настройки IP на ТД или RADIUS-сервер
- Несовпадение порта аутентификации
- Неудачный запрос к LDAP

**РИСУНОК 15.25** Точки отказа—зона 1 решения проблем 802.1X/EAP



Первые три возможных точки отказа находятся между аутентификатором и RADIUS-сервером. Аутентификатор и сервер аутентификации подтверждают друг друга общим секретом [*shared secret*]. Наиболее распространенная ошибка в связи с RADIUS в том, что общий секрет набран неправильно или на RADIUS сервере или на ТД, работающей как аутентификатор.

Вторая широко распространенная ошибка в связи с RADIUS - это просто неправильные настройки IP сети. ТД должна знать корректный IP адрес RADIUS сервера. Аналогично, RADIUS сервер должен быть настроен на IP адреса каждой ТД или контроллера БЛВС, работающих как аутентификаторы. Некорректные настройки IP приведут к ошибкам в установлении связи.

Третья точка отказа между аутентификатором и сервером аутентификации - это несовпадение портов аутентификации RADIUS. Порты UDP 1812 и 1813 определены в качестве отраслевых стандартных портов, используемых для RADIUS аутентификации и учета [*accounting*]. Однако, некоторые старые RADIUS сервера могут использовать UDP порты 1645 и 1646. UDP порты 1645 и 1646 теперь редко используются, но иногда показываются на старых RADIUS серверах. Хотя это и не распространенная точка отказа, если порты аутентификации не совпадают между RADIUS сервером и ТД, процесс аутентификации не пройдет.

Финальная точка отказа на стороне серверов - это ошибка LDAP запроса между RADIUS сервером и базой данных LDAP. Стандартная доменная учетная запись может быть использована для LDAP запроса; однако, если учетная запись устарела или если есть проблема со связью между RADIUS сервером и LDAP сервером, весь процесс аутентификации 802.1X/EAP не состоится.



## Пример из Реальной Жизни

### Какие инструменты могут быть использованы для решения проблем с 802.1X/EAP связью с сервером?

Хорошая новость в том, что доступно несколько ресурсов по решению проблем в зоне 1. Несколько производителей БЛВС предлагают встроенные диагностические инструменты для тестирования связи между аутентификатором и RADIUS-сервером, и связь с LDAP. В зависимости от производителя БЛВС и архитектуры, аутентификатор может быть или точкой доступа, или контроллером БЛВС. Как показано на Рисунке 15.26, стандартная доменная учетная запись и пароль могут использоваться для проверки связи RADIUS и EAP.

Также доступно несколько программных утилит для тестирования серверной или тыловой [backend] связи 802.1X/EAP. EAPTest - это коммерческая утилита по тестированию, доступная для macOS. Больше информации можно найти на [www.ermitacode.com/eaptest.html](http://www.ermitacode.com/eaptest.html). RADLogin - это бесплатная утилита для тестирования для платформ Windows и Linux. Больше информации можно найти на [www.iea-software.com/products/radlogin4.cfm](http://www.iea-software.com/products/radlogin4.cfm). Логи (logs) RADIUS сервера и базы данных LDAP также являются великолепным ресурсом по решению проблем связи между серверами при решении проблем 802.1X/EAP. В худшем случае, может понадобится проводной анализатор протоколов для записи(перехвата) RADIUS пакетов. Многие из этих инструментов тестирования могут также быть использованы для решения проблем с параметрами (атрибутами) RADIUS, которые могут использоваться во время аутентификации 802.1X/EAP для управления доступом на основе ролей [role-based access control (RBAC)].

**РИСУНОК 15.26** Инструмент диагностики серверной связи для 802.1X/EAP

RADIUS Test

Send a RADIUS Access-Request message from the Aerohive device to a RADIUS authentication server or an Accounting-Request message to a RADIUS accounting server.

RADIUS Server  Select a Server

Enter a Server

Aerohive RADIUS Client

Network Connectivity Test  RADIUS Authentication Server

RADIUS Supplicant Credentials  
Note: To test the authentication process for a valid supplicant, enter the user name and password for a user account on the RADIUS authentication server.

User Name or Barcode\*

Password or PIN\*

RADIUS Accounting Server

## Зона 2: Проблемы с Сертификатом Клиента [Supplicant]

Если все тыловые[backend] связи между аутентификатором и RADIUS-сервером работают надлежащим образом, то решение проблем 802.1X/EAP должно перенаправить фокус на Зону 2. Простыми словами, виновник - клиент [supplicant]. Проблемы с клиентом[supplicant] обычно крутятся вокруг или проблем с сертификатами или проблем с клиентскими параметрами[credential]. Давайте взглянем на Рисунок 15.27.

Заметьте, что RADIUS сервер отвечает и, следовательно, подтверждает, что тыловая связь, т.е. связь с серверами, в порядке. Также обратите внимание, что процесс согласования [negotiation] SSL туннеля стартует и финиширует успешно. Это диагностическая запись или лог(log) 802.1X/EAP подтверждает, что сертификационный обмен был успешен и что SSL/TLS туннель успешно был создан, чтобы защитить клиентские параметры [supplicant credentials].

**РИСУНОК 15.27** Успешное создание SSL/TLS туннеля

```
Send message to RADIUS Server(10.5.1.129): code=1 (Access-Request) identifier=100
RADIUS: SSL negotiation, send server certificate and other message
Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=109
Sending EAP Packet to STA: code=1 (EAP-Request) identifier=3 length=280
received EAP packet (code=2 id=3 len=208) from STA: EAP Response-PEAP (25)
Send message to RADIUS Server(10.5.1.129): code=1 (Access-Request) identifier=110
RADIUS: SSL connection established
Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=110
Sending EAP Packet to STA: code=1 (EAP-Request) identifier=4 length=65
received EAP packet (code=2 id=4 len=6) from STA: EAP Response-PEAP (25)
Send message to RADIUS Server(10.5.1.129): code=1 (Access-Request) identifier=111
RADIUS: SSL negotiation is finished successfully
Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=111
Sending EAP Packet to STA: code=1 (EAP-Request) identifier=5 length=43
received EAP packet (code=2 id=5 len=59) from STA: EAP Response-PEAP (25)
Send message to RADIUS Server(10.5.1.129): code=1 (Access-Request) identifier=112
RADIUS: PEAP inner tunneled conversion
```

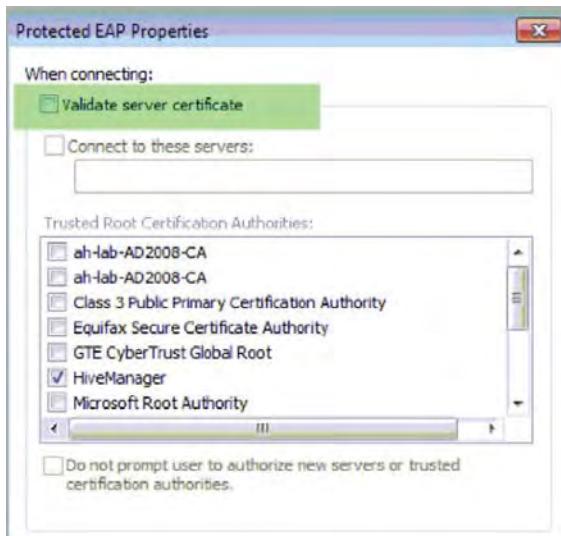
Рисунок 15.28 показывает диагностический лог (диагностическую запись) 802.1X/EAP, где вы можете видеть, что процесс согласования SSL начался и серверный сертификат отправлен от RADIUS сервера к клиенту [supplicant]. Однако, SSL/TLS туннель не создан, и аутентификация EAP не состоялась. Если SSL/TLS туннель не может быть установлен, то это показатель, что есть какая-то проблема с сертификатами.

**РИСУНОК 15.28** Безуспешное создание SSL/TLS туннеля

```
Rx assoc req (rss= 95dB)
IEEE802.1X auth is starting (at if=wifi0.1)
Sending EAP Packet to STA: code=1 (EAP-Request) identifier=0 length=5
received EAP packet (code=2 id=0 len=16) from STA: EAP Response-Identity (1),
Send message to RADIUS Server(10.5.1.129): code=1 (Access-Request) identifier=1
RADIUS: EAP start with type peap
Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=50
Sending EAP Packet to STA: code=1 (EAP-Request) identifier=1 length=6
received EAP packet (code=2 id=1 len=105) from STA: EAP Response-PEAP (25)
Send message to RADIUS Server(10.5.1.129): code=1 (Access-Request) identifier=51
RADIUS: SSL negotiation, receive client hello message
Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=51
Sending EAP Packet to STA: code=1 (EAP-Request) identifier=2 length=1024
received EAP packet (code=2 id=2 len=6) from STA: EAP Response-PEAP (25)
Send message to RADIUS Server(10.5.1.129): code=1 (Access-Request) identifier=52
RADIUS: SSL negotiation, send server certificate and other message
Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=52
Sending EAP Packet to STA: code=1 (EAP-Request) identifier=3 length=280
received EAP packet (code=2 id=3 len=6) from STA: EAP Response-PEAP (25)
Send message to RADIUS Server(10.5.1.129): code=1 (Access-Request) identifier=53
RADIUS: SSL negotiation, send server certificate and other message
Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=53
Sending EAP Packet to STA: code=1 (EAP-Request) identifier=4 length=6
Sta(at if=wifi0.1) is de-authenticated because of notification of driver
```

Обычно вы можете подтвердить, что проблема с сертификатом существует, путем редактирования клиентских настроек программы подключения к Wi-Fi [supplicant client software settings] и времененным отключением проверки сертификата сервера, как показано на Рисунке 15.29. Если аутентификация EAP успешна, после временного отключения проверки сертификата сервера, то вы можете быть уверены в том, что есть проблема с применением сертификатов в структуре 802.1X/EAP. Пожалуйста, заметьте, что это не исправление проблемы, а простой способ подтверждения, что существует какая-то проблема с сертификатом.

**РИСУНОК 15.29** Подтверждение сертификата сервера



Целый диапазон проблем с сертификатами может быть причиной того, что SSL/TLS туннель не может быть успешно создан. Самые распространенные проблемы с сертификатами:

- Корневой сертификат ЦС [root CA certificate] установлен в некорректное хранилище сертификатов.
- Выбран некорректный корневой сертификат.
- Сертификат сервера устарел.
- Корневой сертификат ЦС [root CA certificate] устарел.
- Некорректные настройки часов клиента [supplicant]

Нужно, чтобы корневой сертификат ЦС [root CA certificate] был установлен в хранилище Доверенных Корневых Центров Сертификации [Trusted Root Certificate Authorities] клиентского [supplicant] устройства. Типовая ошибка - это установка корневого сертификата ЦС [root CA certificate] в место по-умолчанию, которое является обычным персональным хранилищем машины на Windows. Еще одна распространенная ошибка - это выбор некорректного корневого сертификата ЦС [root CA certificate] в настройках клиента [supplicant]. SSL/TLS туннель не установится, потому что некорректный корневой сертификат ЦС [root CA certificate] не сможет подтвердить сертификат сервера. Цифровые сертификаты также основаны на времени, и типовая проблема в том, что сертификат сервера просрочен. Хотя это и не распространено,

корневой сертификат ЦС [root CA certificate] также может быть просрочен. Настройки времени на клиенте [supplicant] могут быть некорректны и предшествовать созданию любого из сертификатов.

Так как все возможные точки отказа включают сертификаты, то решение проблем с сертификатами в 802.1X/ EAP в зоне 2 может быть трудным. Кроме того, существует еще больше потенциальных проблем с сертификатами. Может быть некорректная настройка сертификата сервера на RADIUS сервере. Другими словами, проблема с сертификатом находится обратно в зоне 1 решения проблем. А что если развернут аутентификационный протокол EAP-TLS? EAP-TLS требует предоставление сертификата клиентской стороной в дополнение к сертификату сервера. Клиентские сертификаты добавляют дополнительный уровень возможных решений проблем с сертификатами на клиенте [supplicant], а также в развернутой частной инфраструктуре Инфраструктуры Открытых Ключей [PKI -Public Key Infrastructure].

Последнее усложнение может привести к неудаче туннелированной аутентификации. Выбранный протокол EAP уровня 2 должен совпадать на клиенте [supplicant] и сервере аутентификации. Например, аутентификация не удастся, если PEAPv0 (EAP-MSCHAPv2) выбран на клиенте [supplicant], в то время как PEAPv1 (EAP-GTC) настроен на RADIUS сервере. Хотя SSL/TLS туннель все же может быть создан, внутренний туннельный протокол аутентификации не совпадёт и аутентификация не состоится. Хотя возможна одновременная работа нескольких видов EAP поверх одной и той же структуры 802.1X, EAP протоколы должны совпадать и на клиенте [supplicant] и на сервере аутентификации.

## Зона 2: Проблемы с Клиентскими Параметрами [Supplicant Credential]

Если вы можете подтвердить, что у вас нет никаких проблем с сертификатами и SSL/TLS туннель действительно установлен, то проблемы клиента [supplicant] - это сбой с учетными данными [credential]. Рисунок 15.30 показывает запись диагностики 802.1X/ EAP, где RADIUS сервер отклоняет учетные данные клиента [supplicant credentials]. Возможны следующие проблемы с учетными данными клиента:

- Истек срок пароля или учетной записи пользователя [user account]
- Неправильный пароль
- Учетная запись пользователя отсутствует в LDAP
- Учетная запись устройства не присоединена к домену Windows.

**РИСУНОК 15.30** RADIUS сервер отклоняет учетные данные клиента.

```
RADIUS: SSL connection established
Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=127 length=123
Sending EAP Packet to STA: code=1 (EAP-Request) identifier=5 length=65
received EAP packet (code=2 id=5 len=6) from STA: EAP Reponse-PEAP (25)
Send message to RADIUS Server(10.5.1.129): code=1 (Access-Request) identifier=128 length=176
RADIUS: SSL negotiation is finished successfully
Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=128 length=101
Sending EAP Packet to STA: code=1 (EAP-Request) identifier=6 length=43
received EAP packet (code=2 id=6 len=43) from STA: EAP Reponse-PEAP (25)
Send message to RADIUS Server(10.5.1.129): code=1 (Access-Request) identifier=129 length=213
RADIUS: PEAP inner tunneled conversion
Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=129 length=117
Sending EAP Packet to STA: code=1 (EAP-Request) identifier=7 length=59
received EAP packet (code=2 id=7 len=91) from STA: EAP Reponse-PEAP (25)
Send message to RADIUS Server(10.5.1.129): code=1 (Access-Request) identifier=130 length=261
RADIUS: PEAP Tunneled authentication was rejected. NTLM auth failed for logon failure (0xc0000000)
Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=130 length=101
Sending EAP Packet to STA: code=1 (EAP-Request) identifier=8 length=43
received EAP packet (code=2 id=8 len=43) from STA: EAP Reponse-PEAP (25)
Send message to RADIUS Server(10.5.1.129): code=1 (Access-Request) identifier=131 length=213
RADIUS: rejected user 'user' through the NAS at 10.5.1.129.
Authentication is terminated (at if=wifi0.1) because it is rejected by RADIUS server
Sending EAP Packet to STA: code=4 (EAP-Failure) identifier=8 length=4
Sta(at if=wifi0.1) is de-authenticated because of notification of driver
```

Если пользовательские учетные данные не существуют в базе данных LDAP или у учетных данных кончился срок действия, то аутентификация не пройдет. Если на клиенте [supplicant] не применены функции единого входа [single sign-on], то всегда есть вероятность, что пароль пользователя домена мог быть неправильно набран конечным пользователем.

Еще одна распространенная ошибка в том, что Wi-Fi клиент был ошибочно настроен на аутентификацию устройства, а RADIUS сервер был настроен только для аутентификации пользователей. На Рисунке 15.31, вы видите диагностическую запись, которая ясно показывает, что RADIUS серверу были отправлены учетные данные устройства, а не пользовательские учетные данные. RADIUS сервер ожидал пользовательскую учетную запись, и, следовательно, отклонил учетные данные устройства, потому что никаких учетных записей устройства не были настроены для подтверждения. В случае с Windows, учетные данные устройства основаны на значении *Идентификатора Системы [System Identifier (SID)]*, которые хранятся на компьютере домена Windows, после присоединения к Windows домену с Active Directory.

**РИСУНОК 15.31** Ошибки аутентификации устройства

```
Send message to RADIUS Server(10.5.1.129): code=1 (Access-Request) identifier=151 length=203,
RADIUS: SSL negotiation, send server certificate and other message
Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=151 length=340
Sending EAP Packet to STA: code=1 (EAP-Request) identifier=4 length=280
received EAP packet (code=2 id=4 len=17) from STA: EAP Response-PEAP (25)
Send message to RADIUS Server(10.5.1.129): code=1 (Access-Request) identifier=152 length=214,
RADIUS:
RADIUS: rejected user 'host/TRAINING-PC16.ah-lab.local' through the NAS at 10.5.1.129.
Authentication is terminated (at if=wifi0.1) because it is rejected by RADIUS server
Sending EAP Packet to STA: code=4 (EAP-Failure) identifier=4 length=4
Sta(at if=wifi0.1) is de-authenticated because of notification of driver
```

Конечно, администратор БЛВС всегда может убедиться, что все хорошо с клиентской сессией 802.1X/EAP. Всегда помните, что побочным продуктом процесса EAP является создание парных мастер ключей [pairwise master key (PMK)], которые рассылаются обменом сообщений при 4x Стороннем Рукопожатии. Рисунок 15.32 показывает завершение процесса EAP; PMK отправлен ТД от RADIUS сервера. Затем процесс 4x-Стороннего Рукопожатия начинает динамически создавать парный временный ключ [pairwise transient key (PTK)], который уникален между радиомодулями ТД и клиентским устройством. Когда 4x-Стороннее Рукопожатие завершилось, ключи шифрования установлены, и подключение на уровне 2 выполнено. Виртуальный управляемый порт на аутентификаторе открыт для этого Wi-Fi клиента. Теперь клиент может продолжить далее на более высоких уровнях и получить IP адрес. Если клиент не получит IP адрес, то это сетевая проблема, а, следовательно, это не проблема Wi-Fi.

**РИСУНОК 15.32** 4x-Стороннее Рукопожатие

```
Receive message from RADIUS Server: code=2 (Access-Accept) identifier=125
PMK is got from RADIUS server (at if=wifi0.1)
Sending EAP Packet to STA: code=3 (EAP-Success) identifier=5 length=4
Sending 1/4 msg of 4-Way Handshake (at if=wifi0.1)
Received 2/4 msg of 4-Way Handshake (at if=wifi0.1)
Sending 3/4 msg of 4-Way Handshake (at if=wifi0.1)
Received 4/4 msg of 4-Way Handshake (at if=wifi0.1)
PTK is set (at if=wifi0.1)
Authentication is successfully finished (at if=wifi0.1)
IP 10.5.10.100 assigned for station
station sent out DHCP REQUEST message
DHCP server sent out DHCP ACKNOWLEDGE message to station
DHCP session completed for station
```

Последнее, что нужно рассмотреть при решении проблем 802.1X/EAP это параметры (атрибуты) RADIUS. Атрибуты RADIUS могут быть использованы во время аутентификации 802.1X/EAP для контроля доступа на основе ролей [role-based access control], предоставляя индивидуальные настройки для разных групп пользователей или устройств. Например, разным группам пользователей могут быть назначены разные VLANы, даже если они подключаются к одному и тому же 802.1X/EAP SSID. Если настройки атрибутов RADIUS не совпадают на аутентификаторе и RADIUS сервере, пользователям может быть присвоена роль по-умолчанию или VLAN по-умолчанию. В худшем случае, несовпадение параметров RADIUS может привести к отказу в аутентификации.

## Решение проблем с VPN

VPNs теперь используются редко в качестве первичного метода безопасности для корпоративных БЛВС. Иногда, IPsec VPN может использоваться для обеспечения конфиденциальности для канала связи через беспроводной мост 802.11 точка-точка. Однако, IPsec VPNs все еще широко используется для подключения удаленных офисов филиалов к головному офису по каналам WAN. VPNs также используются для решений для удаленных работников, чтобы продлить корпоративную Wi-Fi сеть в дома сотрудников. Хотя канал связи VPN от-места-до-места [site-to-site VPN link] не обязательное решение по безопасности БЛВС, может потребоваться, чтобы беспроводной пользовательский трафик, который начинается на удаленном объекте, проходил через VPN туннель. Большинство производителей БЛВС также предлагают возможности VPN в своих портфелях решений. Например, БЛВС может предложить решение VPN, где пользовательский трафик будет туннелирован от удаленной ТД или БЛВС маршрутизатора филиала до серверного шлюза VPN. Также часто используются сторонние VPN решения.

Создание IPsec VPN туннелей включает две фазы, называемых фазами *Межсетевого Обмена Ключей* [*Internet Key Exchange (IKE)*]:

**IKE Фаза 1** Две конечные точки VPN аутентифицируют друг друга и договариваются о материале ключей. Результатом является шифрованный туннель, используемый Фазой 2 для согласования безопасных ассоциаций Безопасной Инкапсуляции Полезной Нагрузки [*Encapsulating Security Payload (ESP)*].

**IKE Фаза 2** Две конечные точки VPN используют безопасный туннель, созданный на Фазе 1, для согласования безопасных ассоциаций ESP [*ESP security associations (SAs)*]. ESP SAs используются для шифрования пользовательского трафика, который проходит между конечными точками.

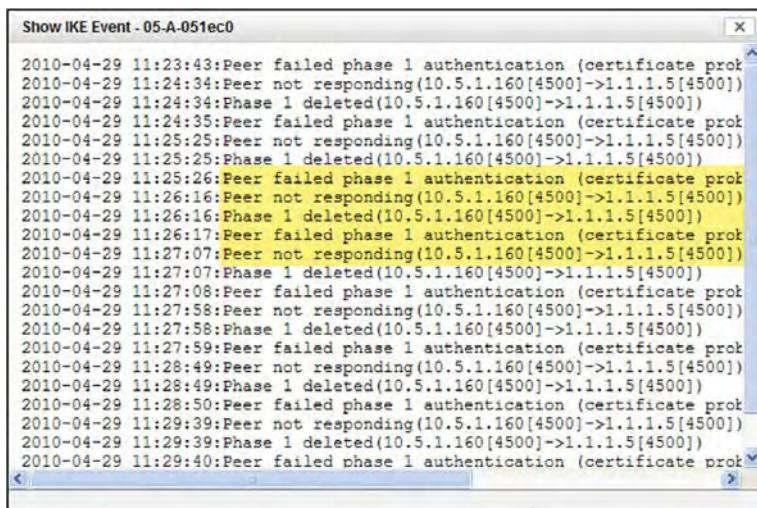
Хорошая новость в том, что любое качественное решение VPN предлагает диагностические инструменты и команды для решения проблем обоих IKE фаз. Вот некоторые из распространенных проблем, которые могут произойти, если IKE Фаза 1 не получилась:

- Проблемы с Сертификатом
- Некорректные сетевые настройки
- Некорректные настройки NAT на внешнем межсетевом экране.

Рисунок 15.33 показывает результаты команды диагностики IKE Фазы 1, выполненных на VPN сервере. IPsec использует цифровые сертификаты во время Фазы 1. Если IKE Фаза 1 не проходит из-за проблем с сертификатом, убедитесь, что у вас правильно установлены корректные сертификаты на конечных точках VPN. Также помните, что

сертификаты основаны на времени. Очень часто, проблема с сертификатами во время IKE Фазы 1 - это просто некорректные настройки часов на обоих конечных точках VPN.

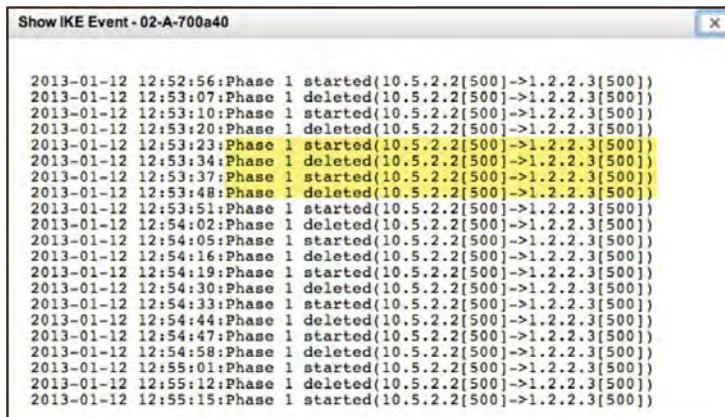
**РИСУНОК 15.33** IPsec Фаза 1—ошибка сертификата



На Рисунке 15.34 вы видите результаты команды диагностики IKE Фазы 1, выполненной на VPN сервере, которые показывают возможную сетевую ошибку из-за некорректной настройки. IPsec использует частные IP адреса для туннельной связи, а также использует внешние IP адреса, которые обычно являются публичными IP адресами межсетевых экранов. Если происходит ошибка IKE Phase как показанная на Рисунке 15.34, проверьте настройки внутренних и внешних IP адресов на VPN устройствах. Если используется внешний межсетевой экран, также проверьте настройки *Сетевой Трансляции Адресов* [*Network Address Translation (NAT)*]. Еще одна распространенная сетевая проблема, которая приводит к отказу в установке VPN - это то, что нужные на межсетевом экране порты заблокированы. Убедитесь, что следующие порты открыты на каждом межсетевом экране, через которые может пройти VPN туннель:

- UDP 500 (IPsec)
- UDP 4500 (NAT Transversal)

**РИСУНОК 15.34** IPsec Фаза 1—сетевая ошибка



Если вы можете подтвердить, что IKE Фаза 1 успешна, а VPN все равно не устанавливается, то вероятнее всего IKE Фаза 2 является виновницей. Вот некоторые из распространенных проблем, которые могут происходить, если IKE Фаза не проходит:

- Несовпадающие наборы преобразований между клиентом и сервером (алгоритм шифрования, хэш алгоритм, и так далее)
- Смесь решений разных производителей

Рисунок 15.35 показывает успешные результаты команды диагностики IKE Фазы 2, выполненной на VPN сервере. Если эта команда показывает сбой, обязательно проверьте настройки и шифрования и хэш на конечных точках VPN. Проверьте другие настройки IPSec, такие как *режим туннеля [tunnel mode]*. Вам нужно проверить, что все настройки совпадают на обоих концах. Проблемы IKE Фазы 2 часто происходят, когда на противоположных сторонах VPN туннеля используются разные производители VPN. Хотя IPSec - это основанный на стандартах набор протоколов, смешение решений разных VPN производителей часто приводит к большему решению проблем.

**РИСУНОК 15.35** IPsec Фаза 2—Успех

```

Show IPsec SA - 02-A-066600

SA(Security Association) information as following:

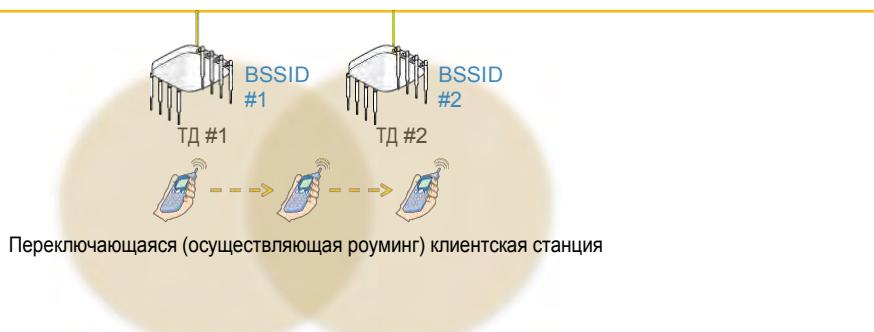
IPsec Security Association Information:
10.5.1.165 [4500] 1.2.1.2 [4500]
tunnel-id: 2
esp-udp modetunnel spi=158846310(0x0977cd66) reqid=0(0x00000000)
Encryption: aes-cbc
Authentication: hmac-sha1
seq=0x00000000 replay=4 flags=0x20000000 state=mature
created: Jul 12 12:48:37 2011 current: Jul 12 12:51:31 2011
diff: 174(s) hard: 3600(s) soft: 2880(s)
last: Jul 12 12:48:37 2011 hard: 0(s) soft: 0(s)
current: 2880(bytes) hard: 0(bytes) soft: 0(bytes)
current: 20(pkts) hard: 0(pkts) soft: 0(pkts)
failed: 0(pkts) replay: 0(pkts) replay window: 0(pkts)
sadb seq=1 pid=944 refcnt=0

1.2.1.2 [4500] 10.5.1.165 [4500]
tunnel-id: 2
esp-udp modetunnel spi=216804365(0x0d0ab08d) reqid=0(0x00000000)
Encryption: aes-cbc
Authentication: hmac-sha1
seq=0x00000000 replay=4 flags=0x20000000 state=mature
created: Jul 12 12:48:37 2011 current: Jul 12 12:51:31 2011
diff: 174(s) hard: 3600(s) soft: 2880(s)
last: Jul 12 12:48:37 2011 hard: 0(s) soft: 0(s)
current: 2880(bytes) hard: 0(bytes) soft: 0(bytes)
current: 20(pkts) hard: 0(pkts) soft: 0(pkts)
failed: 0(pkts) replay: 0(pkts) replay window: 0(pkts)
sadb seq=1 pid=944 refcnt=0

```

## Решение проблем Роуминга

Мобильность - это вся суть в доступе к беспроводной сети. Клиентам 802.11 нужна возможность незаметного переключения между точками доступа без прерывания сервиса и деградации производительности. Как показано на Рисунке 15.36, бесшовный роуминг стал еще более важным за последние годы из-за распространения ручных персональных Wi-Fi устройств таких, как смартфоны и планшеты.



Наиболее распространенные роуминговые проблемы являются результатом или плохих клиентских драйверов или плохого дизайна БЛВС. Очень распространенная *проблема залипшего клиента [sticky client problem]* - это когда клиентская станция остается подключенной к своей изначальной ТД и не переключается на новую ТД, которая ближе и имеет более сильный сигнал. Проблема залипшего клиента часто является результатом расположения ТД в непосредственной физической близости с уровнями мощности передачи, которые слишком высоки. Проблема залипшего клиента и другие проблемы с производительностью роуминга обычно можно избежать надлежащим проектированием БЛВС и обследованиями места. Хороший проект роуминга фиксирует определение надлежащего первичного покрытия и вторичного покрытия с точки зрения клиента, как обсуждалось в Главе 13.

Клиентские станции, а не точка доступа, решают переключаться или нет между точками доступа. Некоторые производители могут вовлекать точку доступа или контроллер БЛВС в решение о роуминге, но в конечном счете клиентская станция инициирует процесс роуминга с кадра запроса на переассоциацию. Метод, которым клиентская станция решает переключаться, зависит от уникальных порогов, определенных производителем клиентского радиомодуля 802.11. Роуминговые пороги обычно определяются RSSI и SNR; однако, другие переменные, такие как процент ошибок и повторных передач, также могут принимать участие в решении о роуминге. Клиентские станции, которые поддерживают 802.11k могут получать отчеты о соседях от 802.11k-совместимых ТД, которые предоставляют клиентским станциям дополнительные данные так, что они могут принимать более лучшие решения. Поддержка 802.11k становится значительно важной в сегодняшних сложных радио средах.

Роуминговые проблемы будут происходить если нет достаточного дублирующего вторичного покрытия. Отсутствие вторичного покрытия, фактически, создает роуминговую мертвую зону, и связь может даже временного пропасть. С другой стороны, слишком много вторичного покрытия также вызовет проблемы с роумингом. Например, клиентская станция может оставаться ассоциированной с исходной ТД и не подключаться ко второй точке доступа, даже если станция прямо под второй точкой доступа. Как ранее упоминали, это называется, как проблема залипшего клиента.

Слишком много потенциальных ТД, слышимых клиентом, могут также привести к ситуации, в которой клиентское устройство постоянно переключается туда-сюда между двумя или более ТД на разных каналах. Если клиентская станция может также слышать дюжину ТД на одном канале с очень сильными сигналами, то произойдет деградация производительности из-за служебной информации при борьбе за среду.

Производительность роуминга имеет прямую связь с безопасностью БЛВС. Каждый раз, когда клиентская станция переключается, должны генерироваться новые ключи шифрования между ТД и клиентским радиомодулями через 4-х Стороннее Рукопожатие.

При использовании безопасности 802.1X/EAP, роуминг может быть особенно доставляющим заботы для VoWiFi и приложений, чувствительных ко времени. Из-за множественного обмена кадрами между сервером аутентификации и клиентом [supplicant], аутентификация 802.1X/EAP может занимать 700 миллисекунд (мс) или больше для того, чтобы аутентифицировать клиента. VoWiFi требует переключения с ТД на ТД в 150 мс или меньше, чтобы избежать деградации качества голоса, или еще хуже, обрыва соединения.

Следовательно, требуется более быстрое, безопасное роуминговое переключение от ТД к ТД.

Изменения в среде БЛВС также могут доставить головные боли о роуминге.

Радиоинтерференция всегда будет влиять на производительность беспроводной сети и также может сделать роуминг проблематичным. Очень часто новые конструкции в здании влияют на покрытие БЛВС и создают новые мертвые зоны. Если физическая среда, где развернута БЛВС, изменяется, то проект покрытия тоже может потребовать изменений. Всегда является хорошей идеей проводить контрольное обследование, чтобы отслеживать изменения в модели покрытия и проверять бесшовную мобильность.

Решение проблем роуминга путем использования анализатора протоколов является сложным из-за того, что обмен сообщениями при преассоциации при роуминге происходит на нескольких каналах. Например, для того, чтобы решить проблему клиентского роуминга между каналами 1, 6 и 11, вам понадобятся три отдельных анализатора протоколов на трех отдельных ноутбуках, которые будут производить три отдельные записи кадров. Как показано на Рисунке 15.37, три USB радиомодуля можно настроить на запись кадров на каналах 1, 6 и 11 одновременно. Все три радиомодуля подключаются к USB хабу и сохраняют записи кадров всех трех каналов в единый файл записи с временными метками. Несколько производителей анализаторов БЛВС предлагают многоканальные мониторинговые возможности и для 2,4 ГГц и для 5 ГГц полос частот. История роуминга клиента БЛВС также может быть собрана с лог-файлов ТД и визуализирована в решениях сетевого управления БЛВС.

#### РИСУНОК 15.37 Многоканальный мониторинг и анализ



Издательство Sybex Publishing's Учебное Руководство Сертифицированный Профессионал Беспроводной Безопасности: Экзамен CWSP-205, 2ое Издание (2016) [CWSP—Certified Wireless Security Professional Study Guide: Exam CWSP-205, 2nd Edition (2016)] посвятило целую главу быстрому безопасному роумингу [fast secure roaming], такому как гибкое (или оппортунистическое) кэширование ключей [opportunistic key caching (OKC)] и быстрый переход BSS [fast BSS transition (FT)]. И OKC и FT производят роуминговое переключение почти за 50 мс даже когда выбрано решение безопасности 802.1X/EAP.

И ОКС и FT используют механизмы распределения ключей так, чтобы роуминговые клиенты не должны были бы переаутентифицироваться каждый раз при переключении. ОКС теперь считается устаревшим методом быстрого безопасного роуминга. Механизмы роуминга FT определенные и в 802.11g и в Voice-Enterprise [Голосовая связь для Предприятий] считаются стандартными. Большинство ТД производителей корпоративного БЛВС теперь сертифицированы для Голосовой связи для Предприятий [Voice-Enterprise] Wi-Fi Альянсом. Пожалуйста, обратите внимание, что любые клиентские устройства, которые произведены до 2012 года просто не поддерживают работу 802.11k/r/v. Хотя большая часть устаревших клиентских устройств не поддерживает возможностей Голосовой связи для Предприятий [Voice-Enterprise], число клиентов, которые поддерживают, растет и становится более распространенным.

Большинство роуминговых проблем, связанных с безопасностью, основаны на том факте, что многие клиенты просто не поддерживают ни ОКС ни быстрый BSS переход [fast BSS transition (FT)]. Поддержка с клиентской стороны для любого устройства, которое будет использовать голосовые приложения и 802.1X/EAP является критичной. Надлежащее планирование и подтверждение поддержки со стороны клиента и ТД для ОКС и FT будет необходимым. Рисунок 15.38 показывает результаты диагностической команды, которые показывают роуминговый кэш точки доступа.

Этот тип диагностической команды может проверить, что РМК были пересланы между точками доступа. В этой ситуации, включена Голосовая Связь для Предприятия [Voice Enterprise] на ТД и поддерживается на клиентском радиомодуле. Вы можете проверить MAC адрес клиента [supplicant] и аутентификатора, а также PMKR0 и держателя [holder] PMKR0. Всегда помните, что клиент [supplicant] должен также поддерживать Голосовую связь для Предприятия [Voice Enterprise] и функции 802.11r; иначе, клиент [supplicant] будет переаутентифицироваться каждый раз при клиентском роуминге.

#### **РИСУНОК 15.38** Роуминговый кэш

```
sh roam cache mac b844:d90e:006e
Supplicant Address(SPA): b844:d90e:006e
PMK(1st 2 bytes): n/a
PMKID(1st 2 bytes): n/a
Session time: -1 seconds
(-1 means infinite)
PMK Time left in cache: 3581
PMK age: 1040
Roaming cache update interval: 60
last time logout: 1221 seconds ago
Authenticator Address: MAC=9c5d:122e:c124, IP=172.16.255.93
Roaming entry is got from neighbor AP: 9c5d:122e:c124
PMK is got(Flag): Locally
Station IP address: 172.16.255.90 (from DHCP)
Station hostname: Davids-iPhone
Station default gateway: 172.16.255.1
Station DNS server: 172.16.255.1
Station DHCP lease time: 85349 seconds
Hops: 0
WPA key mgmt: 64
R0KH: 9c5d:1263:6464
R0KH IP: 172.16.255.94
PMKR0 Name: 19D2*
```

Как ранее упоминалось, включение механизмов Голосовой связи для Предприятия [Voice-Enterprise] на точке доступа может в действительности создать проблемы с подключением для устаревших клиентов. Когда на точке доступа настроен FT, ТД будет широко вещать кадры управления с новыми информационными элементами. Например, *информационный элемент домена мобильности* [*mobility domain information element (MDIE)*] будет во всех кадрах маяках [beacon] и ответов на зондирующий запрос [probe response]. К сожалению, драйвера некоторых старых устаревших клиентских радиомодулей могут не суметь обработать новый информационный элемент в этих кадрах управления. Результат – что устаревшие клиенты могут испытывать проблемы с подключением, когда ТД настроена на FT. Всегда тестируйте парк устаревших клиентов, когда настраиваете ТД для быстрого BSS перехода. Если проблемы с подключением появились, рассмотрите использование отдельного SSID для устройств с быстрым BSS переходом [fast BSS transition]. Помните, однако, что каждый SSID потребляет эфирное время из-за служебной информации кадров управления на уровне 2. Лучшее решение – обновление парка ваших устройств на устройства, которые поддерживают Голосовую Связь для Предприятий [Voice-Enterprise].

Так как беспроводные сети 802.11 обычно интегрируются в уже существующую проводную топологию, то часто нужно пересечение границ уровня 3, особенно в больших корпоративных установках. Единственный способ поддержать связь более высокого уровня при пересечении подсетей Зего уровня – это предоставить решение по роумингу на Зем уровне [*layer 3 roaming*]. Когда клиенты переключаются в новую подсеть, должен быть создан туннель Универсальной Маршрутизируемой Инкапсуляции [Generic Routing Encapsulation (GRE)] в исходную подсеть так, чтобы клиент БЛВС мог сохранить свой исходный IP адрес. Как показано на Рисунке 15.39, основные производители БЛВС предлагают диагностические инструменты и команды для проверки того, что туннели роуминга Зего уровня успешно созданы.

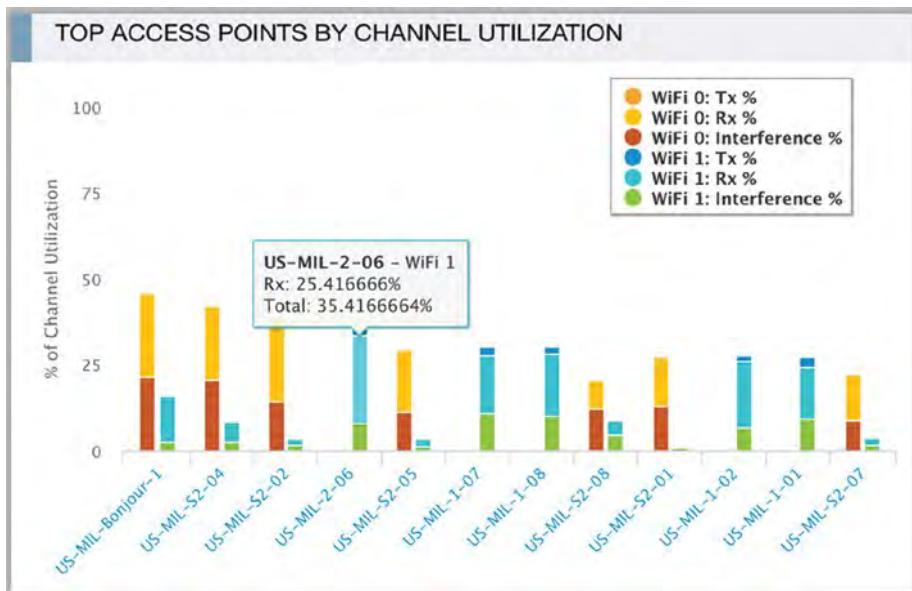
**РИСУНОК 15.39** GRE туннель

## Утилизация Канала

Важная статистика при решении проблем производительности в БЛВС – это утилизация канала [*channel utilization*], как показано на Рисунке 15.40. Помните, что радиоволны – это общая среда, и что радиомодули 802.11 должны по очереди передавать на любом

Wi-Fi канале. Если канал перенасыщен передачами 802.11, по производительности будет нанесен негативный удар. Когда они не передают, радиомодули и ТД и клиента 802.11 слушают канал каждые 9 микросекунд на предмет и передач 802.11 и передач не-802.11.

**РИСУНОК 15.40** Утилизация канала



Несколько хороших порогов по утилизации канала в реальной жизни включают следующие:

- 80 процентов утилизации канала наносит удар по всем передачам данных 802.11.
- 50 процентов утилизации канала наносит удар по видео трафику.
- 20 процентов утилизации канала наносит удар по голосовому трафику.

Мониторинг и решение проблем утилизации канала является важным из-за восприятия производительности Wi-Fi сети конечными пользователями. Типовой звонок в поддержку - это жалоба пользователя на то, что Wi-Fi медленный. Если утилизация канала более 80 процентов, то Wi-Fi действительно медленный. Ненадлежащий дизайн БЛВС, с ненадлежащим планированием каналов очень часто ведут к CCI, которая является причиной высокой утилизации канала. Перенасыщение клиентами и приложениями с широкими полосами могут потреблять очень много эфирного времени на канале, вот почему надлежащее планирование емкости канала так важно. Как вы узнали из Главы 13, слишком большое количество широкого вещания SSID, низкие базовые скорости передачи данных на ТД, и масса устаревших клиентов, все являются виновниками потребления эфирного времени, что влияет на утилизацию канала.

Информационный элемент QBSS, находящийся в кадрах 802.11 маяка [beacon] и ответа на зондирующий запрос [probe response], отправленных ТД, является хорошим индикатором утилизации канала, с точки зрения радиомодуля ТД. Информация, находящаяся в информационном элементе QBSS, как показано на Рисунке 15.41, часто используется

решениями мониторинга у производителей БЛВС и другими приложениями для визуализации утилизации канала в форме графиков или таблиц. Крупные корпоративные заказчики в основном полагаются на возможности мониторинга/решения проблем с точки зрения радиомодуля внутри точки доступа. Радиостатистика, собранная из входящей клиентской радиопередачи, также может центрально мониториться. Информация, собранная с точки зрения радиомодуля ТД.

**РИСУНОК 15.4.1** Информационный элемент QBSS

▼ QBSS Load	Stations: 6, Channel Utilization: 48%
Element ID:	11
Length:	5 bytes
Station Count:	6
Channel Utilization:	124 (48%)
Available Admission Capacity:	0

В действительности, самый лучший вид радиосети всегда будет с точки зрения клиента, вот почему обследование при проектировании БЛВС и контрольное обследование так важны. Один из подходов, который используют некоторые производители БЛВС уровня предприятий, это использовать сенсорные ТД [sensor AP] в месте размещения клиентских устройств, когда они подключаются [log into] к другим ТД как клиентские устройства и затем проверяют состояние сети. Но учтите, что клиенты имеют разную приемную чувствительность, а радиомодули в ТД обычно более чувствительны. Централизованный мониторинг и диагностика с использованием радиомодуля ТД - обычно хорошее начало, но при решении клиентских проблем может понадобиться собрать дополнительную информацию с точки зрения клиента.

Медленная производительность и узкие места в полосе могут действительно быть результатом плохого дизайна Wi-Fi, а плохая утилизация канала - является хорошим индикатором проблем с производительностью Wi-Fi. Однако, причина, по которой конечному пользователю кажется, что Wi-Fi медленный, не имеет ничего общего с БЛВС или утилизацией канала. Узкие места в полосе очень часто находятся на проводной сети, из-за слабого дизайна проводной сети. Узкое место в полосе номер один - это обычно канал подключения к сети широкого охвата [WAN uplink] на любом удаленном месте. Но помните, что всегда сначала винят Wi-Fi, независимо от нехватки полосы на сети широкого охвата [WAN].

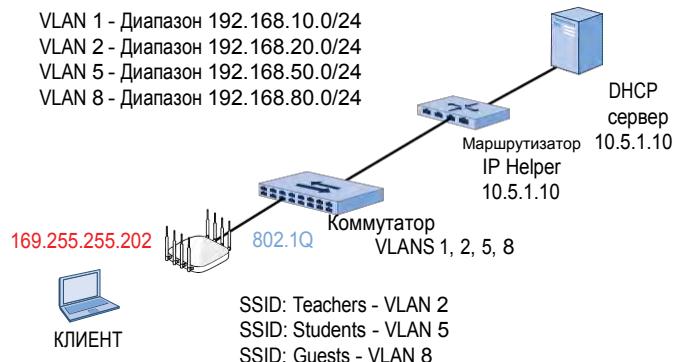
## Решение проблем Уровней 3-7

Хотя эта глава сфокусирована на решении проблем БЛВС на уровнях 1 и 2 модели OSI, решение проблем на верхних уровнях может оказаться необходимым. БЛВСы очень часто обвиняют в возникновении проблем, которые на самом деле существуют в проводной сети на более высоких уровнях. Если сотрудники не могут подключиться к корпоративной БЛВС, то сотрудники обвиняют БЛВС, даже если реальная проблема где-то еще в корпоративной сети. Если можно определить, что эта проблема не проблема уровня 1 или уровня 2, то обычно это сетевая проблема или проблема с приложением.

Хорошая новость в том, что много производителей БЛВС предлагают инструменты решения проблем высоких уровней, которые доступны в системах управления сетью (NMS), контроллерах БЛВС, или из командной строки ТД. Типовой звонок в поддержку - это пользователи, жалующиеся на то, что у них есть подключение к Wi-Fi, но нет подключения к сети. Если вы уже определили, что проблемы - не проблема Wi-Fi, переходите выше по стеку OSI к уровню 3, чтобы проверить IP связность.

Рассмотрите диаграмму школьной БЛВС, показанной на Рисунке 15.42. ТД установлена в школе и передает три SSID, по одному для учителей (teachers), студентов(students) и гостей(guests). Учительский SSID связан с VLAN 2, студенческий SSID связан с VLAN 5, а гостевой SSID связан с VLAN 8. Интерфейс управления ТД связан с VLAN 1. Все четыре VLAN проходят с тэгами (tag) через 802.1Q транк между ТД и коммутатором доступа. Все четыре VLANа связаны с соответствующими подсетями, и все IP адреса предоставляются из определенных диапазонов на сетевом DHCP сервере.

**РИСУНОК 15.42** Схема школьной БЛВС



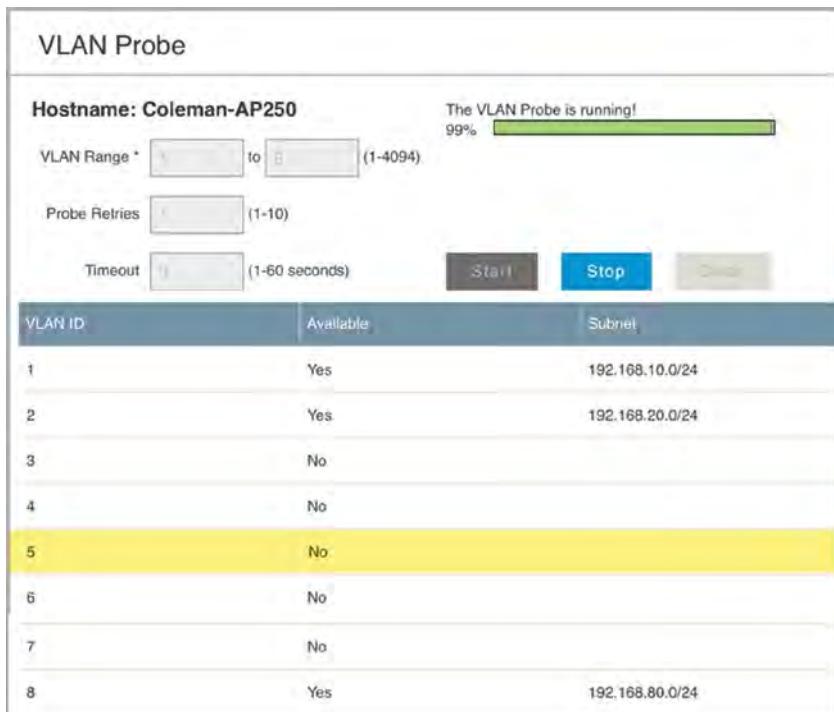
Как ранее упоминалось, типовой звонок в поддержку - это пользователь, жалующийся, что у них есть Wi-Fi подключение, но они не могут подключиться к сети. В этом сценарии, студент должен получить IP адрес из сети 192.168.50.0/24. Быстрая проверка определила, что студент подключен к соответствующему SSID; однако, студент получает автоматический частный IP адрес [automatic private IP address (APIPA)] из диапазона 169.254.0.0–169.254.255.255. Это будет вашим первым индикатором, что эта проблема наиболее вероятно - это проблема проводной части сети.

Производители БЛВС могут предложить инструменты диагностики, которые могут быть использованы для получения отчета, работают ли VLANы на проводной сети, а также подсети в каждом VLANe. Как показано на Рисунке 15.43, администратор может выбрать ТД, чтобы провести зондирование по назначенному диапазону VLANов. Обратите внимание, что VLAN 5 (студенческий VLAN) не доступен.

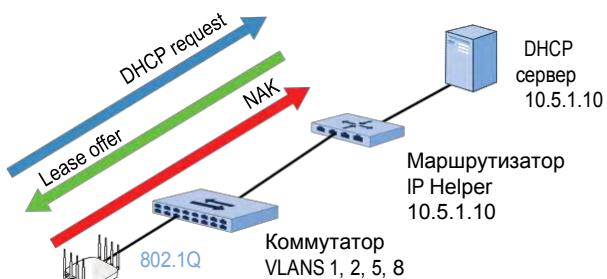
Инструменты диагностики используют возможность интерфейса управления любой точки доступа отправлять DHCP запрос, как показано на Рисунке 15.44. Если зондирование началось, то интерфейс управления ТД отправляет несколько DHCP запросов по всем указанным VLANам. Каждый DHCP запрос отправляется по транку 802.1Q в проводную сеть. Если DHCP запрос наконец достиг DHCP сервера, то предложение по аренде IP адреса [lease offer] отправляется обратно к ТД. Интерфейсу управления ТД не нужен еще один IP адрес, следовательно, отрицательное подтверждение [negative acknowledgment (NAK)] отправляется обратно на DHCP сервер. Если DHCP предложение по аренде IP адреса

достигает ТД, то это не проблема проводной сети. Однако, если DHCP предложение по аренде IP адреса [DHCP lease offer] не достигает ТД, то это абсолютно точно проблема на проводной стороне, и диагностическое зондирование покажет отрицательный результат.

**РИСУНОК 15.43** Зондирование VLAN



**РИСУНОК 15.44** Зондирование DHCP



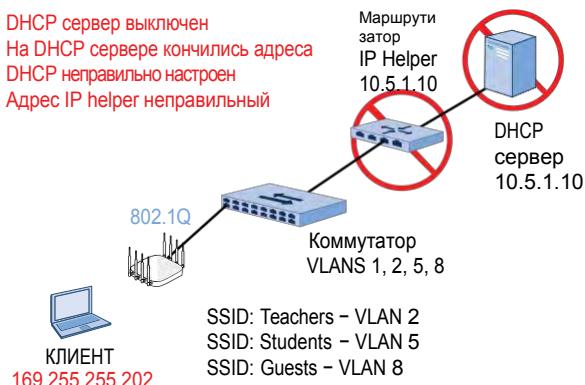
SSID: Teachers – VLAN 2

SSID: Students – VLAN 5

SSID: Guests – VLAN 8

Как показано на Рисунке 15.45, есть две типовые точки отказа - это вышестоящий маршрутизатор [upstream router] и DHCP сервер. DHCP запросы используют широковещательный адрес, следовательно нужно настроить адрес IP Helper (DHCP-Relay) на вышестоящем маршрутизаторе [upstream router], чтобы преобразовать DHCP запрос в односторонний пакет [unicast packet]. Если на маршрутизаторе нет корректного адреса IP Helper, то DHCP запрос никогда не достигнет DHCP сервера. DHCP сервер является более вероятной точкой отказа. DHCP сервер может сломаться, диапазон адресов может быть некорректно настроен, или у сервера могут просто кончиться адреса для выдачи в аренду.

**РИСУНОК 15.45** DHCP отказы со стороны проводной сети



Хотя эти две точки определенно возможны, но наиболее вероятный виновник - это коммутатор доступа, как показано на Рисунке 15.46. Почти в 90 процентов случаев, проблема в неправильно настроенном коммутаторе доступа. VLANы могут быть не настроены на коммутаторе, VLANы могут быть без тэгов(меток) на транковом 802.1Q порту, или порт может быть неправильно настроен на точке доступа.

**РИСУНОК 15.46** Неправильно настроенный коммутатор



Даже, если клиенты БЛВС успешно получают IP адреса, это все еще может быть сетевыми проблемами уровня 3. Команды `ping` и `traceroute/tracert` являются вашими следующими шагами по диагностике вашей сети. Команда `ping` и другие команды по опросу сети доступны в каждой клиентской операционной системе (OS), а также на OS, работающей на ТД, коммутаторах и маршрутизаторах.

Если вы определили, что на уровне 3 на сети нет проблем, вы можете начать исследовать уровни 4-7. Скотт Адамс [Scott Adams] создал мини комикс про Дилберта в 2013 году, где все винят межсетевой экран во всех сетевых проблемах:

<http://dilbert.com/strip/2013-04-07>. Это мультяшное отражение реальной жизни, потому что некорректно настроенные политики межсетевого экрана могут заблокировать TCP и UDP порты. В дополнение к возможностям межсетевого экрана с отслеживанием состояний [stateful firewall], производители БЛВС начали встраивать межсетевые экраны, способные проводить *глубокий анализ пакетов* [*deep packet inspection (DPI)*], в точки доступа или контроллеры БЛВС. DPI обеспечивают видимость приложений, используемых по БЛВС, а межсетевые экраны уровня Приложений могут блокировать конкретное приложение или группу приложений. Где бы не был развернут межсетевой экран в вашей сети, если есть подозрение на проблему на верхних уровнях, то может понадобится просмотреть лог-файлы межсетевого экрана.

Всегда помните, что точка доступа - это беспроводной портал ко всей сетевой инфраструктуре. Если Wi-Fi сеть - не проблема, то нужно решать проблему на уровнях 3-7.

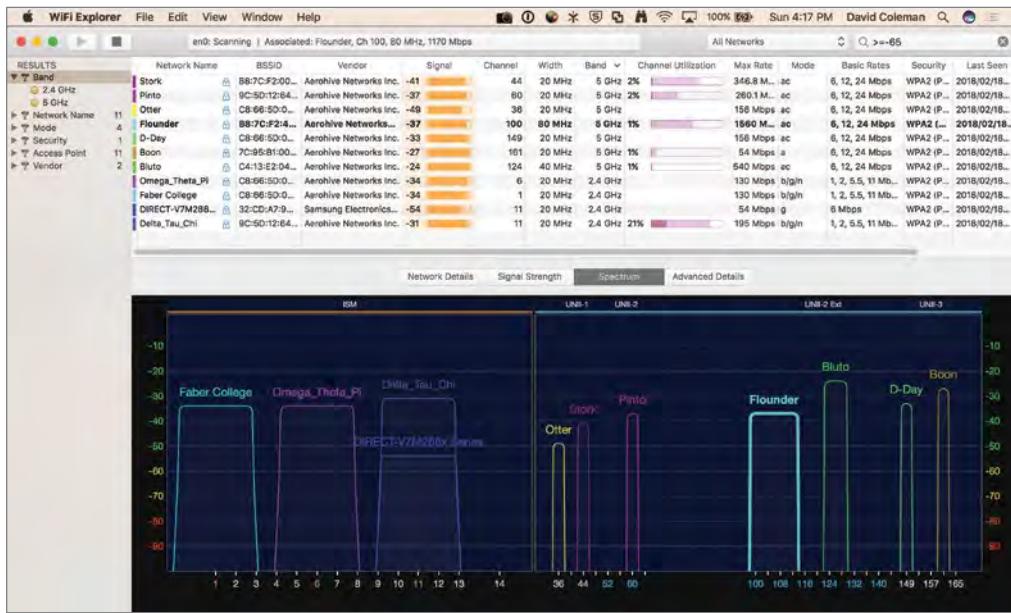
## Инструменты для решения проблем БЛВС

Хотя производители БЛВС предоставляют значительные возможности по диагностике из их систем управления сетью, каждый профессионал БЛВС обычно имеет при себе большой массив инструментов в своем персональном наборе инструментов по решению проблем БЛВС. Этот раздел описывает некоторые из доступных инструментов.

### Приложения по обнаружению БЛВС

Чтобы начать решать проблемы БЛВС, вам нужна клиентская сетевая карта (NIC) 802.11 и приложение по обнаружению БЛВС, например, WiFi Explorer (показанный на Рисунке 15.47). Приложения по обнаружению БЛВС являются быстрым и легким способом, который даёт вам широкий обзор существующей БЛВС. Инструменты обнаружения БЛВС находят существующие Wi-Fi сети путем отправки кадров пустого зондирующего запроса [null probe request] и прослушиванием кадров 802.11 ответов на зондирующий запрос [probe response] и маяков [beacon], отправленных ТД. Хотя инструмент обнаружения БЛВС не даст вам глубокий анализ, который вам может предоставить анализатор протоколов, вы можете собрать много полезной информации. Например, инструмент обнаружения БЛВС может немедленно сказать вам, что включены 80 МГц каналы на ТД и производительность под негативным воздействием. Хороший инструмент обнаружения БЛВС может дать вам быстрый обзор числа передающих ТД и их каналов, размеров каналов, и характеристики безопасности. Другая доступная информация включает силу сигнала, SNR, статистику утилизации канала, и многое другое.

РИСУНОК 15.47 Инструмент обнаружения БЛВС



Существуют многочисленные бесплатные и коммерческие инструменты обнаружения, включая inSSIDer для Windows, WinFi для Windows, Acrylic Wi-Fi для Windows, WiFi Explorer для macOS, и WiFi Analyzer для Android. Вы можете загрузить inSSIDer с [www.metageek.com](http://www.metageek.com), WinFi Pro или Lite с [www.helge-keck.com](http://www.helge-keck.com), Acrylic Wi-Fi Home или Professional с [www.acrylicwifi.com](http://www.acrylicwifi.com), WiFi Explorer или WiFi Explorer Pro с [www.intuitibits.com](http://www.intuitibits.com), и WiFi Analyzer с [bit.ly/WiFIAnalyze](http://bit.ly/WiFIAnalyze).

## Анализаторы Спектра

Анализаторы спектра - это измерительные устройства из области частот, которые могут измерять амплитуду и частотное пространство электромагнитных сигналов. Рисунок 15.48 изображает анализатор спектра на основе ПК, который использует USB-адаптер, который может мониторить спектры 2,4 ГГц и 5ГГц. Анализатор спектра компании МетаГик [MetaGeek's ([www.metageek.com](http://www.metageek.com))] Wi-Spy использовался для определения источников радиоинтерференции, показанных ранее в этой главе на Рисунках 15.3-15.5. Анализатор спектра - это инструмент диагностики уровня 1, который наиболее часто используется для обнаружения источников радиоинтерференции, которая исходит от не-802.11 передатчиков.

**РИСУНОК 15.48** Анализатор спектра 2,4 ГГц и 5 ГГц на основе ПК - Wi-Spy DBx

## Анализаторы Протоколов

Анализаторы протоколов обеспечивают видимость сети в точности того, какой трафик проходит по сети. Анализаторы протоколов перехватывают и сохраняют сетевые пакеты, предоставляя вам декодирование протоколов каждого перехваченного пакета, которое является читаемым выводом на экран, показывающее индивидуальные поля и значения для каждого пакета. Сила анализатора протокола в том, что он позволяет вам видеть общение между различными сетевыми устройствами на многих уровнях модели OSI. Анализ протокола иногда является единственным способом решить сложную проблему. Доступно много коммерческих анализаторов протоколов БЛВС, например: TamoSoft's CommView for WiFi ([www.tamos.com](http://www.tamos.com)), LiveAction's Omnipeek ([www.liveaction.com](http://www.liveaction.com)), а также популярный бесплатный анализатор протоколов Wireshark ([www.wireshark.org](http://www.wireshark.org)).

Проводные анализаторы протоколов часто называются анализаторами пакетов, потому что они используются для решения проблем с IP пакетами, которые передаются по проводным сетям. Помним, что если проблема - не проблема уровня 1 и не проблема уровня 2, то Wi-Fi не виноват. Анализ пакетов проводного трафика часто необходим для решения проблем, которые происходят на уровнях 3-7.

Анализ протоколов БЛВС в основном используется для просмотра обмена кадров 802.11 на 2ом уровне между ТД и клиентскими устройствами. Радиомодули Wi-Fi взаимодействуют путем обмена кадрами 802.11 на MAC подуровне. В отличие от многих проводных сетевых стандартов, таких как IEEE 802.3, который использует один тип кадров данных, стандарт IEEE 802.11 определяет три основных типа кадров:

управления, контроля и данных. Эти типы кадров далее подразделяются на несколько подтипов, как вы узнали из Главы 9. При использовании анализатора протоколов БЛВС для просмотра кадров при работе 802.11, обычно вы не смотрите на уровня 3-7. Надеемся, весь ваш трафик данных 802.11 зашифрован.

Анализатор протоколов БЛВС и некоторые инструменты по обнаружению БЛВС также могут предоставить обзор некоторой информации уровня 1 и радиостатистики. Заголовки *Радиопрослушки [Radiotap]* предоставляют дополнительную информацию канального уровня [*link-layer*], которая добавляется ко всем кадрам 802.11, когда они перехватываются. Драйвера радиомодулей 802.11 сообщают дополнительную информацию через заголовок Радиопрослушки [*Radiotap header*]. Нужно понимать, что заголовок Радиопрослушки [*Radiotap header*] не является частью формата кадра 802.11. Однако, возможность увидеть дополнительную информацию, такую как сила сигнала, связанная с каждым кадром 802.11, услышанным радиомодулем анализатора протоколов БЛВС, очень полезна. Wi-Fi эксперт Эдриан Гранадос [*Adrian Granados*] дает более детальное объяснение о заголовке Радиопрослушки [*Radiotap header*] в своем блоге ([www.intuitibits.com/2015/04/06/link-layer-header-types](http://www.intuitibits.com/2015/04/06/link-layer-header-types)).

Мы всегда говорим людям, что одна из самых лучших вещей, которую мы делали ранее в нашей Wi-Fi карьере, была самообучение анализу кадров 802.11. Спустя двадцать лет, умение анализировать протокол 802.11 все также важно и неоценимо. Современные анализаторы протоколов БЛВС более надежны, но обмен кадров 802.11 постоянно становится более сложным. По мере того, как новые технологии 802.11, такие как 802.11ax, становятся реальностью, информация внутри кадрового обмена 802.11 создает Wi-Fi мозаику, которую сложно интерпретировать. Не важно насколько много, как вы можете думать, вы знаете об анализе кадров 802.11, вы можете всегда узнать больше.

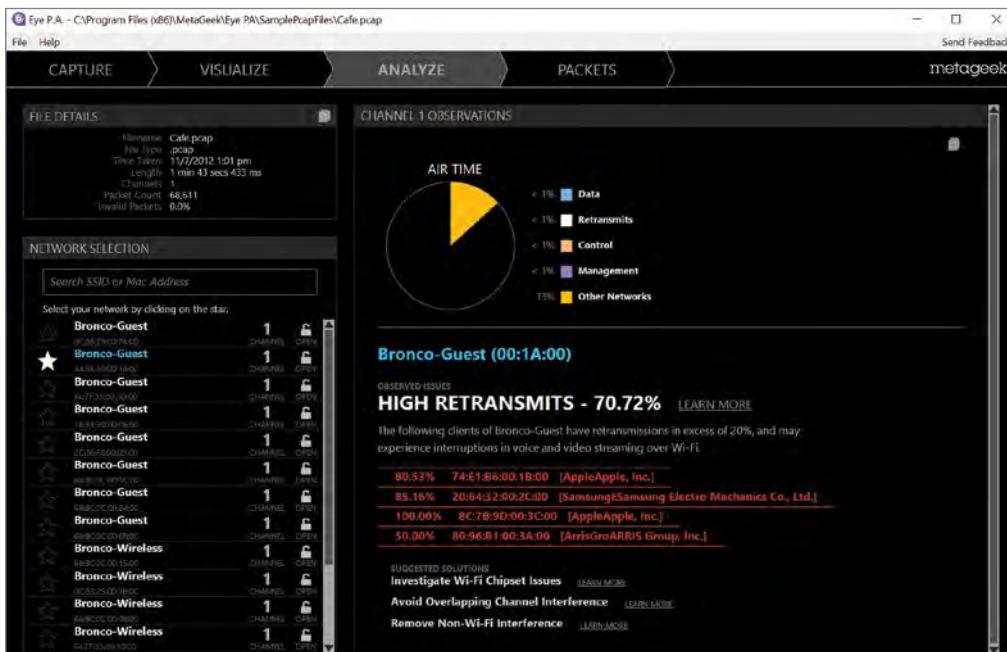
Хотя существует много коммерческих анализаторов протоколов БЛВС, Wireshark ([www.wireshark.org](http://www.wireshark.org)) - с открытым исходным кодом и является инструментом выбора многих профессионалов БЛВС. Авторы этой книги настойчиво рекомендуют два видеокурса, созданных Джеромом Хенри [*Jerome Henry (CWNE #45)*] и Джеймсом Гаррингером [*James Garringer (CWNE #179)*]. Если вы новичок в Wireshark, мы настойчиво рекомендуем учебный курс *Основы WireShark Живые Уроки [WireShark Fundamentals LiveLessons]* (<http://bit.ly/WShark1>), который предлагает почти пять часов инструкций по использованию Wireshark для решения проблем на Ethernet и Wi-Fi сетях и протоколах, которые они передают. Вы узнаете про Wireshark - основы перехвата, настройки фильтрации, опции командной строки, и многое другое.

Если вам нужно более глубокое погружение в анализ 802.11, то мы настойчиво рекомендуем учебный видеокурс *Wireshark для Беспроводной ЛВС Живые Уроки [Wireshark for Wireless LANs LiveLessons]* (<http://bit.ly/WShark2>), который предлагает более восьми часов экспертных инструкций по решению проблем Wi-Fi сетей с использованием WireShark. Девять уроков и под-уроков проведут вас через знакомство с заголовком 802.11 MAC [*802.11 MAC header*], разбором перехваченных кадров, продвинутым инструментам, и распространенными проблемами БЛВС, которые могут быть решены соответствующим анализом.

При использовании анализатора протокола, использование возможностей по фильтрации трафика для фокусировки на сетевом взаимодействии, в котором вы пытаетесь решить проблемы, является необходимым. Справочное руководство по большинству фильтров 802.11, используемых в Wireshark доступно для загрузки по ссылке <http://bit.ly/WFilter>, любезно предоставленной Франсуа Верже [*François Vergès (CWNE #180)*]. Коммерческие анализаторы протоколов имеют более продвинутые возможности по фильтрованию. Любой хороший анализатор протоколов также будет иметь

возможность визуализировать трафик взаимодействий, а также возможно будет способен предоставить интеллектуальную диагностику и предложит шаги по исправлению. Рисунок 15.49 - это снимок экрана с анализатора протокола БЛВС MetaGeek's EyePA, диагностирующего неприемлемый процент повторных передач уровня 2 на ТД, вместе с предлагаемыми шагами по исследованию причины проблемы.

**РИСУНОК 15.49** EyePA анализ и восстановление.



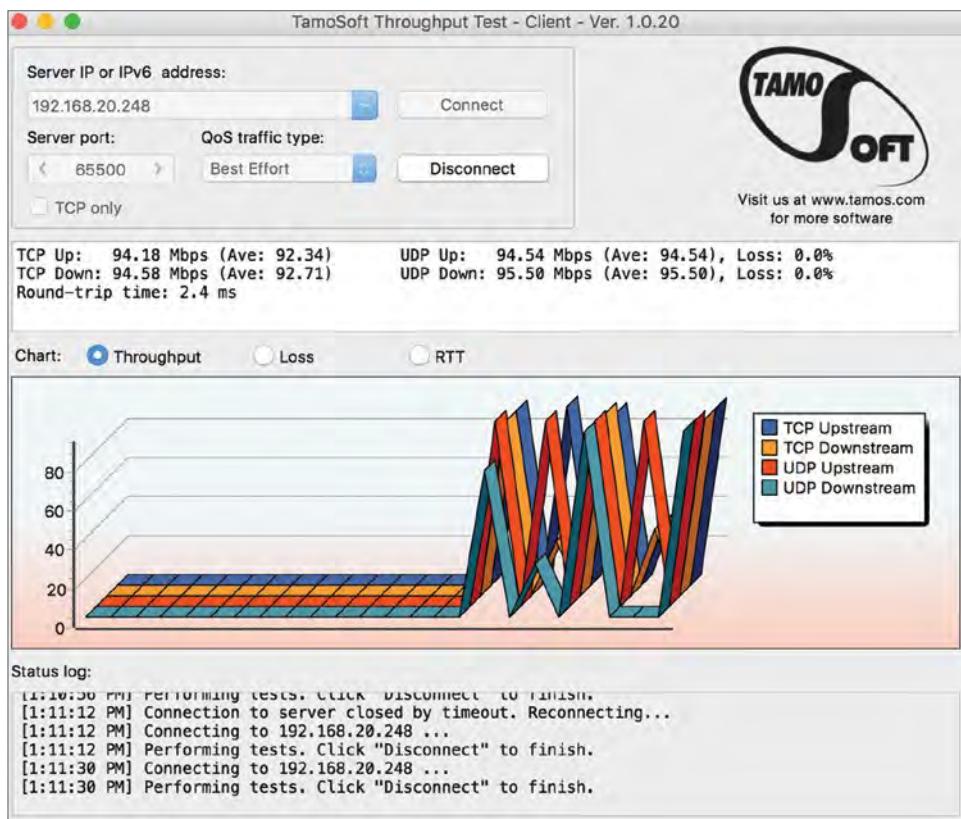
Определение корректного местоположения для размещения сетевого анализатора является существенным шагом в проведении успешного анализа беспроводной сети. Некорректное размещение анализатора протоколов БЛВС может привести к ошибочным заключениям. Например, если вы перехватываете трафик слишком далеко от источника и точки назначения, вы можете увидеть много поврежденных кадров; однако, тот, кто должен получать трафик, может не испытывать какие-либо аномалии с кадрами. Точка доступа действует как центральная точка в беспроводной сети 802.11, а весь трафик должен идти через точку доступа. Производители БЛВС уровня предприятия предлагают прямой перехват пакетов с точек доступа. В таком сценарии, если анализатор сообщает о поврежденных кадрах, то более чем вероятно, что ТД также видит кадры поврежденными.

## Инструменты Проверки Пропускной Способности

Инструменты проверки пропускной способности используются для оценки полосы и производительности пропускной способности сети. Тестеры пропускной способности обычно работают по модели клиент/сервер, чтобы измерить потоки данных между двумя концами или в обоих направлениях. Когда вы проверяете пропускную способность нисходящего канала связи [downlink] БЛВС, клиент 802.11 должен быть настроен в качестве сервера. Когда вы проверяете пропускную способность восходящего канала [uplink] БЛВС клиент 802.11 должен быть настроен в качестве клиента, связывающегося с сервером за ТД. *iPerf* это утилита командной строки с открытым исходным кодом, которая повсеместно используется для

генерирования потоков данных TCP или UDP для проверки пропускной способности. Многие производители БЛВС предлагают iPerf в качестве проверочной утилиты CLI прямо из OS точек доступа или контроллеров БЛВС. Как показано на Рисунке 15.50, ТамоСофт [TamoSoft ([www.tamos.com](http://www.tamos.com))] предлагает бесплатный тестер пропускной способности с графическим интерфейсом, который доступен для Windows, macOS, iOS, и Android клиентов.

**РИСУНОК 15.50** Тестер пропускной способности TamoSoft



При проведении тестирования пропускной способности беспроводного канала связи, всегда помните, что вы тестируете не скорости передачи данных 802.11. В зависимости от сетевых условий БЛВС, агрегированная пропускная способность БЛВС обычно составляет 50 процентов от рекламируемой скорости передачи данных 802.11 из-за обычной служебной информации при борьбе за среду [overhead]. Скорости передачи данных 802.11 – это не пропускная способность TCP. Протокол борьбы за доступ к среде CSMA/CA много потребляет из доступной полосы. В лабораторных условиях, пропускная способность TCP в среде 802.11n/ac составляет 60-70 процентов от скорости передачи данных между одной ТД и одним клиентом. Значения агрегированной пропускной способности значительно меньше в условиях реальных сред с активным участием нескольких клиентов БЛВС, работающих через ТД.

Использование клиент/серверных инструментов по проверке пропускной способности в проводной части сети часто является необходимым. Помните, причина, по которой Wi-Fi кажется медленным для конечного пользователя, часто не имеет ничего общего с БЛВС или утилизацией канала. Узкие места в полосе очень часто находятся на проводной сети из-за

слабого сетевого дизайна. Еще раз, узкое место номер один в ограничении полосы - это обычно канал подключения к распределенной сети [WAN uplink] из удаленного места.

## Стандартные IP Сетевые Команды

Всегда помните, что у вас есть стандартные инструменты для решения сетевых проблем, доступные в различных операционных системах. Каждый знает, что вы всегда начинаете с команды **ping**, самый широко используемый сетевой инструмент для базовой проверки связности между запрашивающим хостом и хостом назначения. Команда **ping** использует *Межсетевой Протокол Контрольных Сообщений* [*Internet Control Message Protocol (ICMP)*] для отправки эхо-пакета хосту назначения и слушая ответ от хоста. Используйте **ping** для проверки IP связности между клиентом БЛВС и локальным сетевым сервером. Используйте **ping** чтобы увидеть может ли клиент БЛВС достичь адрес шлюза по умолчанию. Пинганите [Ping] публичные DNS сервера компании Google - 8.8.8.8, чтобы увидеть есть ли у клиента БЛВС доступ в Интернет через распределенную сеть [WAN].

Другие широко используемые сетевые команды:

**arp** Команда **arp** используется для просмотра кэша *Протокола Определения Адреса* [*Address Resolution Protocol (ARP)*], который ставит соответствие между IP адресами и MAC адресами. Каждый раз, когда стек TCP/IP устройства использует ARP, чтобы определить MAC адрес для IP адреса, он записывает соответствие адресов в кэш ARP для ускорения в будущем поиска ARP. Просмотр кэша ARP на точке доступа часто является полезным при решении проблем.

**tracert/traceroute** Команда **tracert** или **traceroute**, доступная в большинстве операционных систем, нужна для того, чтобы определить подробную информацию о пути к хосту назначения, включая маршрут следования IP пакета, число пролетов между узлами [hop], и время ответа между различными пролетами.

**nslookup** Команда **nslookup** используется для решения проблем с определением адреса в *Системе Доменных Имен* [*Domain Name System (DNS)*]. DNS используется для определения IP адресов по доменным именам. Используйте команду **nslookup** для поиска конкретного IP адреса, связанного с доменным именем. Многие перехватывающие порталы БЛВС [WLAN captive web portals], используемые для гостевого доступа в БЛВС, базируются на перенаправлении DNS запросов. Если перехватывающий портал БЛВС [WLAN captive web portal] внезапно перестанет работать, вам скорее всего нужно заподозрить, что проблема с DNS.

**netstat** Команда **netstat** показывает сетевую статистику для активных TCP сессий и для входящих и для исходящих портов, Ethernet статистику, IPv4 и IPv6 статистику, и другое. Команда **netstat** часто полезна при решении проблем с подозрением на проблемы с приложением и проблемы с межсетевым экраном.

При решении проблем с клиентской стороны БЛВС, эти команды легко доступны из командной строки устройств, работающих на Windows, macOS, или Linux. Многие бесплатные приложения также доступны и для использования на iOS и Android, так, что вы можете получить доступ к этим возможностям решения проблем с мобильных устройств смартфонов и планшетов.

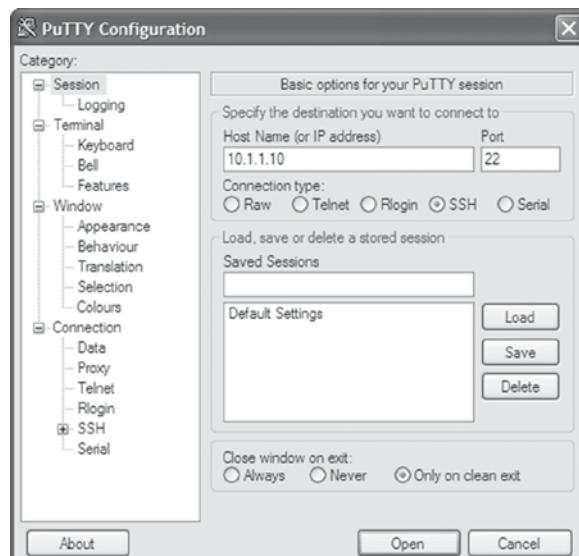
### **Есть ли какие-либо CLI команды для решения проблем радиомодулей клиентов БЛВС?**

Простой ответ - да, в зависимости от операционной системы клиентского устройства БЛВС. Команда `netsh` (сетевая оболочка [network shell]) может быть использована для настройки и решения проблем как с проводным, так и с беспроводным сетевыми адаптерами на компьютерах Windows. Команды `netsh wlan show` покажут детальную информацию о Wi-Fi радиомодуле, используемом компьютером Windows. Например, `netsh wlan show networks` покажет все видимые Wi-Fi сети, которые радиомодуль клиента видит. Сопоставимая утилита командной строки для настройки и решения проблем сетевых адаптеров 802.11 на компьютерах macOS - это инструмент командной строки `airport`. Уделите время для знакомства с командами и `netsh wlan` для Windows и `airport` для macOS. Как и с любой командой CLI, выполните команду `? для просмотра всех опций.`

## **Безопасная Оболочка [Secure Shell]**

При подключении к сетевому оборудованию, такому как точка доступа или коммутатор, потребуется SSH или консольный клиент [serial client]. *Безопасная Оболочка [Secure Shell (SSH)]* используется в качестве безопасной альтернативы Telnet. SSH применяет аутентификацию и шифрование с открытым ключом для всего сетевого трафика между хостом и пользовательским устройством. SSH протоколу назначен стандартный TCP порт 22. Большинство инфраструктурных устройств БЛВС теперь используют вторую версию протокола SSH, называемого SSH2. Что касается политики, то когда устройства БЛВС управляются по CLI, то должны использоваться программы эмуляции терминала с поддержкой SSH2. Рисунок 15.51 показывает экран настройки популярной бесплатной программы PuTTY, которая поддерживает SSH2 и эмуляцию терминала. PuTTY является программой выбора, когда нужно подняться по лесенке и подключиться к консольному порту точки доступа. Кроме того, некоторые операционные системы, такие как macOS, изначально поддерживают SSH из командной строки, или с использованием программы, такой как iTerm2.

**РИСУНОК 15.51** PuTTY—бесплатный SSH и серийный [serial] клиент.



# Итого

Решение проблем БЛВС может быть очень сложным. Большинство решений проблем БЛВС крутится около проблем производительности или проблем с подключением, которые являются результатом ненадлежащего проектирования БЛВС. Однако, из-за постоянно меняющейся радиосреды, неизбежно возникают проблемы с роумингом, скрытыми узлами, и интерференцией. Никогда не забывайте, что Wi-Fi работает на 1ом и 2ом уровнях модели OSI, и помните, что БЛВС всегда будут обвинять не зависимо от того, где находится проблема. Всегда помните про использование передового опыта решения проблем, анализ проблем на разных уровнях модели OSI, и использование всех диагностических инструментов, которые могут быть доступны.

## Темы Экзамена

**Понимать основы решения проблем.** Осознавать важность постановки корректных вопросов и сбор соответствующей информации для определения корня причины проблемы.

**Объяснить где на модели OSI происходят различные проблемы БЛВС.** Помнить, что решение проблем по модели OSI является рекомендованной стратегией. Проблемы с безопасностью БЛВС почти всегда находятся на уровнях 1 и 2. Помните, что большинство проблем с подключением БЛВС также находится на клиентских устройствах, а не на инфраструктуре БЛВС.

**Объяснить, как решать проблемы с аутентификацией PSK.** Понимать, что обычные причины отказа в аутентификации PSK - это проблемы с клиентским драйвером и несовпадением учетных данных для входа. 4-х Стороннее Рукопожатие не состоится, если не состоялась аутентификация PSK.

**Определить несколько точек отказа аутентификации 802.1X/EAP.** Объяснить все потенциальные точки отказа серверных[backend] взаимодействий и возможные клиентские [supplicant] ошибки. Понимать, как анализировать процесс 802.1X/EAP, чтобы точно указать на точку отказа/ошибки.

**Объяснить потенциальные проблемы безопасности БЛВС с роумингом.** Понимать, что и инфраструктура БЛВС и клиенты БЛВС должны поддерживать механизмы быстрого безопасного роуминга [fast secure roaming], такие как Голосовая Связь для Предприятия [Voice-Enterprise].

**Идентифицировать причины проблем уровня 1 в БЛВС.** Понимать, что большинство сетевых проблем обычно находятся на Физическом уровне. Объяснить все проблемы уровня 1, которые часто вызываются плохим дизайном БЛВС, радиоинтерференцией, драйверами радиомодулей, проблемами с прошивками, или проблемами с PoE.

**Понимать, что повторные передачи уровня 2 - это зло.** Распознавать множество причин повторных передач на уровне 2 и их существенные неблагоприятные влияния, когда повторные передачи уровня 2 превышают уровень в 10 процентов.

## Контрольные Вопросы

1. На каком уровне модели OSI происходит большинство сетевых проблем?
  - A. Физическом [Physical]
  - B. Канальном [Data-Link]
  - C. Сетевом [Network]
  - D. Транспортном [Transport]
  - E. Сеансовом [Session]
  - F. Презентационном [Presentation]
  - G. Прикладном [Application]
2. Что может вызвать отказ в аутентификации PSK? (Выберите все, что применимо.)
  - A. Несовпадение пароля
  - B. Просроченный корневой сертификат ЦС [root CA certificate]
  - C. Проблема клиентского драйвера БЛВС
  - D. Просроченная учетная запись LDAP
  - E. Несовпадение шифрования
3. Когда Wi-Fi сеть является фактическим источником проблемы с подключением, безопасностью или производительностью, на каком устройстве БЛВС обычно находится проблема?
  - A. Контроллер БЛВС
  - B. Точка доступа
  - C. Клиент БЛВС
  - D. Сервер управления беспроводной сетью
4. Какие проблемы могут произойти, когда точка доступа внутри помещения передает на полной мощности? (Выберите все, что применимо.)
  - A. Скрытый узел [Hidden node]
  - B. Одноканальная интерференция [Co-channel interference]
  - C. Залипшие клиенты [Sticky clients]
  - D. Межсимвольная интерференция [Intersymbol interference]
  - E. Перестройка по полосам [Band hopping]
5. Один пользователь жалуется, что у его VoWiFi телефона прерывистый звук. Администратор БЛВС заметил, что у пользовательского MAC адреса коэффициент повторов [retry rate] 25 процентов при наблюдении анализатором протоколов. Однако, у всех других пользователей около 5 процентов при наблюдении анализатором протоколов. Какая наиболее вероятная причина этой проблемы?
  - A. Близко/далеко [Near/far]
  - B. Многолучевое распространение [Multipath]

- C. Одноканальная интерференция [Co-channel interference]
  - D. Скрытый узел [Hidden node]
  - E. Низкий SNR [Low SNR]
6. Эндрю Гарсиа, администратор БЛВС, пытается объяснить своему боссу, что БЛВС не является причиной того, что босс Эндрю не может написать в Фейсбуке [Facebook]. Эндрю определил, что проблем нет на уровне 1 и уровне 2 модели OSI. Что следует сказать Эндрю своему боссу? (Выберите лучший ответ.)
- A. Wi-Fi работает только на уровне 1 и уровне 2 модели OSI. БЛВС - не является проблемой.
  - B. Вероятнее всего это сетевая проблема или проблема с приложением.
  - C. Не беспокойтесь, босс, я починю это.
  - D. Почему вы просматриваете Facebook в рабочее время?
7. Каковы некоторые негативные последствия повторных передач уровня 2? (Выберите все, что применимо.)
- A. Уменьшенная зона обслуживания [Decreased range]
  - B. Избыточная служебная информация MAC подуровня [Excessive MAC sublayer overhead]
  - C. Уменьшенная задержка [Decreased latency]
  - D. Увеличенная задержка [Increased latency]
  - E. Джиттер [Jitter]
8. Вам поставили задачу по решению проблемы с клиентским подключением в головном офисе вашей компании. Все ТД и iPad'ы сотрудников настроены на аутентификацию PSK. Сотрудники заметили, что они не могут подключить свои iPad к ТД в приемной основного здания, но могут подключить к другим ТД. Посмотрите на следующий график и опишите причину проблемы.

```
BASIC Rx assoc req (rssi 93dB)
INFO WPA-PSK auth is starting (at if=wifi0.1)
INFO Sending 1/4 msg of 4-Way Handshake (at if=wifi0.1)
INFO Received 2/4 msg of 4-Way Handshake (at if=wifi0.1)
INFO Sending 1/4 msg of 4-Way Handshake (at if=wifi0.1)
INFO Received 2/4 msg of 4-Way Handshake (at if=wifi0.1)
BASIC Sta(at if=wifi0.1) is de-authenticated because of notification of driver
```

- A. Драйвер клиента БЛВС не правильно взаимодействует с OS устройства.
  - B. ТД настроены только на шифрование CCMP. Клиент поддерживает только TKIP.
  - C. Клиент настроен с неправильным паролем WPA2-Personal.
  - D. ТД в приемной настроена с неправильным паролем WPA2-Personal.
9. Вам поставили задачу настроить безопасный БЛВС из 400 ТД в корпоративных офисах. Все ТД и ноутбуки сотрудников на Windows настроены на 802.1X/EAP с использованием PEAPv0 (EAP-MSCHAPv2). Пользовательские доменные учетные данные не могут аутентифицироваться при любой попытке. После просмотра графика, показанного здесь, определите возможную причину проблемы. (Выберите все, что применимо.)

```

Rx assoc req (rss=95dB)
IEEE802.1X auth is starting (at if=wifi0.1)
Sending EAP Packet to STA: code=1 (EAP-Request) identifier=0 length=5
received EAP packet (code=2 id=0 len=16) from STA: EAP Response-Identity (1),
Send message to RADIUS Server(10.5.1.129): code=1 (Access-Request) identifier
RADIUS: EAP start with type peap
Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=50
Sending EAP Packet to STA: code=1 (EAP-Request) identifier=1 length=6
received EAP packet (code=2 id=1 len=105) from STA: EAP Response-PEAP (25)
Send message to RADIUS Server(10.5.1.129): code=1 (Access-Request) identifier
RADIUS: SSL negotiation, receive client hello message
Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=51
Sending EAP Packet to STA: code=1 (EAP-Request) identifier=2 length=1024
received EAP packet (code=2 id=2 len=6) from STA: EAP Response-PEAP (25)
Send message to RADIUS Server(10.5.1.129): code=1 (Access-Request) identifier
RADIUS: SSL negotiation, send server certificate and other message
Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=52
Sending EAP Packet to STA: code=1 (EAP-Request) identifier=3 length=280
received EAP packet (code=2 id=3 len=6) from STA: EAP Response-PEAP (25)
Send message to RADIUS Server(10.5.1.129): code=1 (Access-Request) identifier
RADIUS: SSL negotiation, send server certificate and other message
Receive message from RADIUS Server: code=11 (Access-Challenge) identifier=53
Sending EAP Packet to STA: code=1 (EAP-Request) identifier=4 length=6
Sta(at if=wifi0.1) is de-authenticated because of notification of driver

```

- A. Сетевые настройки на ТД некорректны.
- B. Настройки часов клиента [supplicant] некорректны.
- C. Присутствует несовпадение портов аутентификации между ТД и RADIUS-сервером.
- D. Сетевые настройки на RADIUS-сервере некорректны.
- E. На клиенте [supplicant] выбран некорректный корневой сертификат.
- F. Корневой сертификат просрочен.
10. Сетевой администратор Кофейной Компании Чудо-Щенок звонит на горячую линию поддержки своего производителя БЛВС и сообщает персоналу поддержки, что БЛВС сломана. Персонал поддержки задает заказчику серию вопросов так, чтобы можно было изолировать и идентифицировать причину потенциальной проблемы. Что из перечисленного является типовыми вопросами простого решения проблем [Troubleshooting 101]? (Выберите все что применимо.)
- A. Когда случилась проблема?
- B. Какой ваш любимый цвет?
- C. Что вы ищите?
- D. Повторяется ли проблема или она случилась один раз?
- E. Делали ли вы какие-либо изменения недавно?
11. Корпоративные IT администраторы, Хантер, Райен, и Лиам, собрались вместе, чтобы попытаться решить проблему с недавно установленными телефонами VoWiFi. Выбранное решение безопасности PEAPv0 (EAP-MSCHAPv2) для голосового SSID, на котором также включена поддержка Голосовой связи для Предприятий [Voice-Enterprise] на точке доступа. VoWiFi телефоны безупречно аутентифицируются и голосовые звонки стабильны, когда сотрудники используют устройства за своими столами. Однако, есть провалы в звуке и иногда разъединения, когда сотрудники говорят по VoWiFi телефонам и идут в другие области здания. Какие возможные причины прерывания сервиса для голосовых вызовов, когда сотрудники мобильны? (Выберите все, что применимо)
- A. VoWiFi телефоны должны быть настроены только на аутентификацию PSK, когда требуется роуминг.
- B. VoWiFi телефоны переаутентифицируются каждый раз, когда они переключаются на новую ТД.

- C.** VoWiFi телефоны не используют гибкое кэширование ключей [opportunistic key caching].
- D.** VoWiFi телефоны не поддерживают быстрый BSS переход.
- 12.** Что из следующего является двумя наиболее вероятными причинами проблем с роумингом? (Выберите все, что применимо.)
- A.** Недостаточное вторичное покрытие [Not enough secondary coverage]
- B.** Слишком много вторичного покрытия [Too much secondary coverage]
- C.** Одноканальная интерференция [Co-channel interference]
- D.** Интерференция смежных зон [Adjacent cell interference]
- E.** Скрытый узел [Hidden node]
- 13.** У профессора Перри Корелла есть коммутатор, который совместим с 802.3at. У него есть проблемы с хаотичной перезагрузкой ТД. Что из следующего может быть причиной его проблем?
- A.** Несколько настольных PoE VoIP телефонов включены в тот же Ethernet коммутатор.
- B.** Большинство Ethernet кабелей, идущих от коммутатора до ТД, 90 метров в длину.
- C.** Кабели Ethernet только Категории 5e [Cat 5e]
- D.** Коммутатор поддерживает 1000BaseT, что не совместимо с ТД.
- 14.** Какая команда CLI в Windows может показать клиентский метод аутентификации в БЛВС, способ шифрования, канал, силу сигнала и скорость передачи данных?
- A.** netsh wlan show drivers
- B.** airport -S
- C.** netsh wlan show interfaces
- D.** airport -I
- E.** nslookup
- F.** traceroute
- 15.** Сетевой администратор Корпорации Святой Грааль звонит на горячую линию поддержки своего производителя БЛВС и сообщает персоналу поддержки, что БЛВС больше не работает. Персонал поддержки задает заказчику серию вопросов так, чтобы они могли изолировать и идентифицировать причину потенциальной проблемы. Какие типовые вопросы по простому решению проблем? (Выберите все, что применимо)
- A.** Когда происходит проблема?
- B.** Где происходит проблема
- C.** Проблеме подвержен один клиент или многочисленные клиенты?
- D.** На сколько высокая скорость полета ненагруженной ласточки?

- 16.** Администратор БЛВС Марко Тислер решает проблему с IPSec VPN между БЛВС маршрутизатором удаленного филиала и сервером VPN шлюза в корпоративной штаб-квартире. Марко не может заставить установиться VPN туннель и замечает, что есть ошибка сертификата во время обмена сообщениями IKE Фазы 1. Какая возможная причина этой проблемы? (Выберите все, что применимо)
- A.** VPN сервер в корпоративной штаб-квартире использует шифрование AES-256, а маршрутизатор БЛВС удаленного филиала использует шифрование AES-192.
  - B.** VPN сервер в корпоративной штаб-квартире использует хэш SHA-1 для проверки целостности данных, а маршрутизатор БЛВС удаленного филиала использует MD5 для целостности данных.
  - C.** Корневой сертификат ЦС [root CA certificate], установленный на VPN маршрутизатор БЛВС удаленного филиала, не использовался для подписи серверного сертификата на корпоративном VPN сервере.
  - D.** Настройки часов на корпоративном VPN сервере установлены более ранним числом создания сертификата сервера.
  - E.** Настройки публичного/частного IP адреса неверны на маршрутизаторе БЛВС удаленного филиала.
- 17.** Вам поставили задачу настроить безопасную БЛВС из 600 ТД в корпоративных офисах. Все ТД и ноутбуки сотрудников Google Chromebook настроены на PEAPv0 (EAP-MSCAPv2). Не устанавливается связность для одного из ноутбука сотрудников. После просмотра графика, показанного здесь, определите возможную причину проблемы. (Выберите все, что применимо.)
- ```
Receive message from RADIUS Server: code=2 (Access-Accept) identifier=125
PMK is got from RADIUS server (at if=wifi0.1)
(63)Sending 1/4 msg of 4-Way Handshake (at if=wifi0.1)
(64)Received 2/4 msg of 4-Way Handshake (at if=wifi0.1)
(65)Sending 3/4 msg of 4-Way Handshake (at if=wifi0.1)
(66)Received 4/4 msg of 4-Way Handshake (at if=wifi0.1)
(67)PTK is set (at if=wifi0.1)
(68)Authentication is successfully finished (at if=wifi0.1)
(69)station sent out DHCP REQUEST message
(70)station sent out DHCP REQUEST message
(71)station sent out DHCP REQUEST message
```
- A.** VLAN на коммутаторе доступа настроен некорректно.
  - B.** Учетные записи машин не были присоединены к домену.
  - C.** Сертификат сервера просрочен.
  - D.** Клиент [supplicant] настроен только на аутентификацию пользователя.
  - E.** Корневой сертификат просрочен.
  - F.** У DHCP сервера закончились адреса для раздачи.
- 18.** Что может быть сделано, чтобы решить проблему скрытого узла? (Выберите лучший ответ.)
- A.** Увеличить мощность на точку доступа.
  - B.** Переместить станцию - скрытой узел.
  - C.** Уменьшить мощность на всех клиентских станциях.
  - D.** Устранить препятствие.
  - E.** Уменьшить мощность на станции - скрытом узле.
  - F.** Добавить еще одну ТД

- 19.** Повторные передачи уровня 2 происходят, когда кадры становятся поврежденными. Что является причинами повторных передач уровня 2? (Выберите все, что применимо).
- A.** Высокое SNR
  - B.** Низкое SNR
  - C.** Одноканальная интерференция [Co-channel interference]
  - D.** Радиоинтерференция [RF interference]
  - E.** Интерференция смежных каналов [Adjacent channel interference]
- 20.** Когда вы решаете проблему клиентского подключения у клиента, использующего безопасность 802.1X/EAP, какое первое действие вы должны сделать, чтобы исследовать потенциальную проблему уровня 1?
- A.** Перезагрузить клиента БЛВС.
  - B.** Проверить корневой сертификат ЦС [root CA certificate]
  - C.** Проверить EAP протокол.
  - D.** Выключить и снова включить клиентский сетевой интерфейс радиомодуля.
  - E.** Проверить серверный сертификат.



# Глава 16



## Беспроводные Атаки, Мониторинг Вторжения, и Политика.

---

**В ЭТОЙ ГЛАВЕ ВЫ УЗНАЕТЕ О СЛЕДУЮЩЕМ:**

✓ **Беспроводные атаки**

- Неучтенные[rogue] беспроводные устройства
- Пиринговые (peer-to-peer) атаки
- Прослушивание
- Взлом шифрования
- Атака с переустановкой ключа [KRACK attack]
- Уязвимость KrOOk
- Аутентификационные атаки
- Подмена MAC
- Использование уязвимостей интерфейса управления.
- Беспроводной угон [hijacking]
- Атаки отказа-в-обслуживании (DoS)
- Атаки на оборудование конкретного производителя
- Социальная инженерия

✓ **Мониторинг вторжения**

- Система предотвращения беспроводного проникновения (WIPS)
- Обнаружение неучтенной ТД и уменьшение ее влияния
- Анализаторы спектра

✓ **Политики беспроводной безопасности**

- Общие политики безопасности
- Рабочие политики безопасности
- Соответствие законодательству
- Рекомендации по политикам беспроводной 802.11 безопасности.



В этой главе мы охватим широкое разнообразие атак, которые могут быть запущены против беспроводных сетей 802.11. Некоторые из этих атак могут быть нивелированы путем использования сильного шифрования и решений взаимной аутентификации, которые мы обсуждаем в Главе 17 "802.11 Архитектура Сетевой Безопасности".

Другие атаки, однако, не могут быть предотвращены и могут быть только обнаружены. Следовательно, мы также обсуждаем системы обнаружения беспроводного вторжения, которые могут быть установлены, чтобы увидеть атаки на уровень 1 и на уровень 2. Наиболее важный компонент для безопасной беспроводной сети - это надлежащим образом спланированная и внедренная корпоративная политика безопасности. Эта глава также обсуждает некоторые фундаментальные компоненты политики беспроводной безопасности, которые нужно заложить в основание безопасности Wi-Fi.

## Беспроводные Атаки

Как вы узнали из этой книги, главная функция БЛВС 802.11 - это предоставление портала в проводную сетевую инфраструктуру. Портал должен быть защищен сильными методами аутентификации так, чтобы только законным пользователям и устройствам с соответствующими учетными данными было разрешено иметь доступ к сетевым ресурсам. Если портал защищен не надлежащим образом, то неавторизованные пользователи могут получить доступ к этим ресурсам. Потенциальные риски обнажения этих ресурсов бесконечны. Вторгающийся может получить доступ к финансовым базам данных, корпоративным торговым секретам, или персональной медицинской информации. Сетевые ресурсы могут быть повреждены.

Каковы были бы финансовые затраты для организации, если бы вторгающийся использовал беспроводную сеть в качестве портала для разрушения или выключения VoIP сервера или сервера электронной почты? Если Wi-Fi портал не был защищен, то любой желающий нанести вред мог бы загрузить такие данные, как вирусы, приложения типа Троянского коня, регистраторы нажатия клавиш, или приложения по удаленному управлению. Спамеры уже поняли, что они могут использовать открытые беспроводные шлюзы в интернет, чтобы начать спамерскую активность. Другие нелегальные действия, такие как кража программного обеспечения и удаленный взлом, также могут осуществляться через незащищенный шлюз.

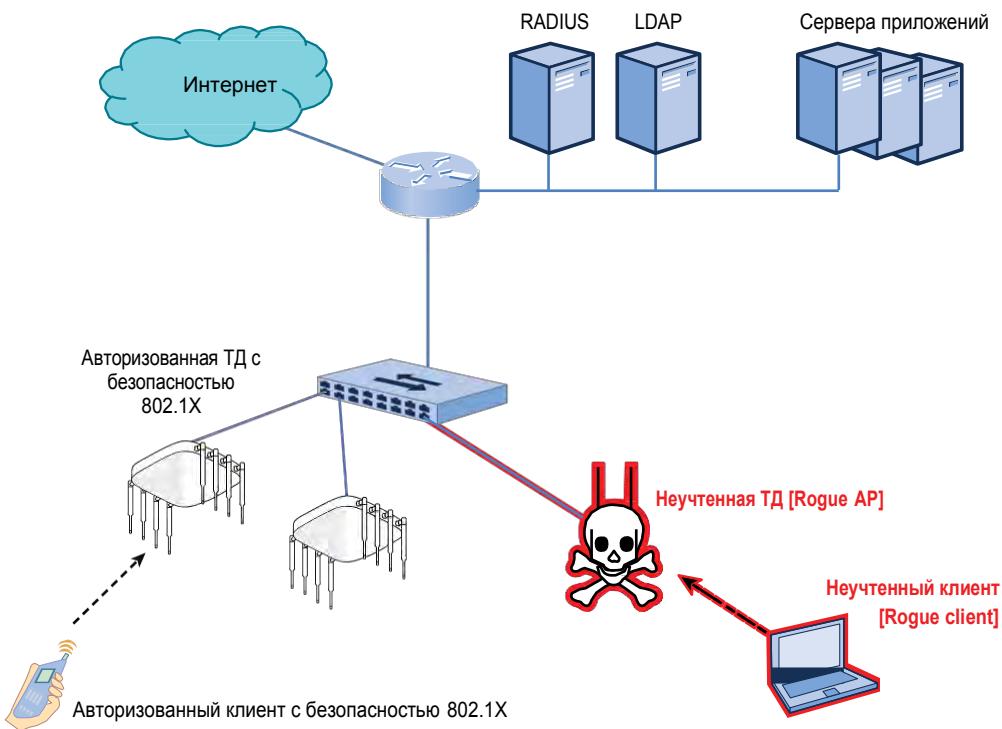
В то время как вторгшийся может использовать беспроводную сеть для атаки на проводные ресурсы, одинаково подвержены риску все беспроводные сетевые ресурсы. Любая информация, которая проходит через эфир, может быть перехвачена и возможно скомпрометирована. Без надлежащей защиты интерфейсы управления оборудования Wi-Fi могут быть доступны. Многие беспроводные пользователи полностью открыты пиринговым [peer-to-peer] атакам. Наконец, всегда существует возможность атак отказа-в-обслуживании [denial-of-service (DoS)]. С соответствующими инструментами любой с болезненной манией может временно выключить Wi-Fi сеть, препятствуя таким образом законным пользователям получать доступ к сетевым ресурсам.

В следующих разделах вы узнаете о многих потенциальных атаках, которые могут быть запущены против беспроводных сетей 802.11.

## Неучтенные беспроводные устройства

Фраза вызывающая больше всего шума в безопасности Wi-Fi всегда была *неучтенная точка доступа [rogue access point]*: - потенциально открытый и незащищенный шлюз прямо в проводную инфраструктуру, которую компания хочет защитить. В главе 17 вы узнаете о решениях аутентификации 802.1X/EAP, которые могут быть установлены, что бы предотвратить неавторизованный доступ. Но как предотвратить установку персоналом своих собственных беспроводных порталов в опорную сеть? Неучтенная точка доступа - это любое неавторизованное Wi-Fi устройство, которое не находится под управлением соответствующих сетевых администраторов. Самая большая угроза безопасности БЛВС - это любой тип неавторизованного неучтенного Wi-Fi устройства, которое подключено к проводной сетевой инфраструктуре, как показано на Рисунке 16.1. Иконка череп и перекрещенные кости является распространенным символом, использующимся для обозначения неучтенных ТД, так же как и пиратов. Любая потребительского-класса Wi-Fi точка доступа или маршрутизатор могут быть включены в действующий порт данных. Неучтенное устройство будет выступать в качестве портала в проводную сетевую инфраструктуру. Так как неучтеннное устройство скорее всего будет настроено без какой-либо аутентификации и авторизации, любой злоумышленник может использовать этот открытый портал для получения доступа к сетевым ресурсам.

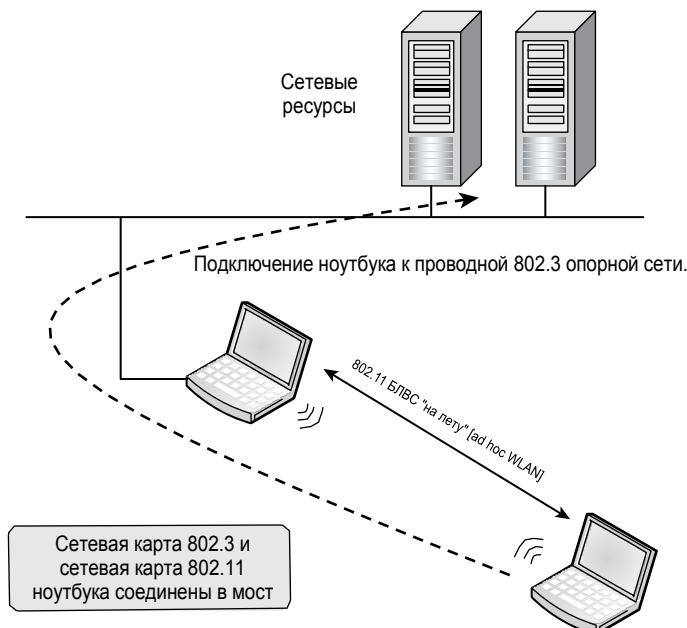
РИСУНОК 16.1 Неучтенная точка доступа



Те, кто чаще всего ответственен за установку неучтенных точек доступа, обычно не являются хакерами; они являются сотрудниками, не осознающими последствия своих действий. Wi-Fi сеть стала встроенной в наше общество, и среднестатистический сотрудник привык к удобству и мобильности, которые предлагает Wi-Fi. В результате, не является не обычным, что сотрудник устанавливает свои собственные беспроводные устройства на рабочем месте, потому что сотрудники полагают, что установка своего беспроводного устройства проще и более надежнее, чем использование корпоративной БЛВС. Проблема в том, что хотя эти самовольно установленные неучтенные точки доступа могут предоставить беспроводной доступ, который желают сотрудники, они часто незащищены. Для доступа к ресурсам нужен только один портал, а многие крупные компании обнаружили буквально десятки неучтенных точек доступа, которые были установлены сотрудниками.

Беспроводные соединения "на лету" [ad-hoc], также могут потенциально предоставить неучтенный[rogue] доступ в корпоративную сеть. Очень часто у сотрудников есть ноутбук или настольный компьютер, включенные в проводную сеть через сетевую Ethernet карту. На том же самом компьютере у сотрудника есть Wi-Fi радиомодуль и устанавливаемое Wi-Fi соединение "на лету" [ad-hoc] с другим сотрудником. Это соединение может быть установлено специально или может быть случайным и образовано как непреднамеренный результат заводских настроек по умолчанию. Как показано на Рисунке 16.2, Ethernet соединение и сетевая интерфейсная Wi-Fi карта [Wi-Fi (NIC)] могут быть объединены в мост; и злоумышленник может попасть в беспроводную сеть "на лету" [ad-hoc], а затем потенциально может направить свой путь в Ethernet соединение и попасть в проводную сеть.

**РИСУНОК 16.2** Мост с БЛВС "на лету" [ad-hoc]



Многие правительственные организации и корпорации запрещают использование сетей "на лету" [ad hoc] на ноутбуках именно по этой причине. Возможность настроить сеть "на лету" [ad hoc] должна быть отключена на большинстве корпоративных устройств. На некоторых компьютерах возможно ограничить использование нескольких сетевых карт [NICs] одновременно. Эта замечательная возможность, которая может предотвратить образование сетей-мостов при этом предоставляя гибкость пользователю. Когда пользователь подключен Ethernet кабелем в ноутбук, беспроводной адаптер автоматически выключается, устранив риск преднамеренного или непреднамеренного образования сетевого моста.

Еще один распространенный тип неучтенного подключения - это беспроводной принтер. Многие принтеры теперь оснащены радиомодулем 802.11 с заводской настройкой в режиме [ad hoc], т.е. образования сети "на лету". Атакующие могут подключиться к этим принтерам с использованием заводских инструментов управления, которые можно загрузить с сайта производителя. Используя эти инструменты, атакующие могут подгрузить свою собственную прошивку на ваш принтер, позволяющую им организовать мост между проводной и беспроводной сетями без использования точки доступа. Многие беспроводные 802.11 видеокамеры систем безопасности также могут взломаны похожим способом.

Как ранее утверждалось, большинство неучтенных ТД устанавливаются сотрудниками, не осознающими последствия своих действий, и любой злоумышленник может использовать эти открытые порталы, чтобы получить доступ. Более того, кроме физической безопасности, ничего не мешает злоумышленнику подключить свою собственную точку доступа Ethernet кабелем в любой работающий порт данных, размещенных на стенах. Позже в этой главе мы обсуждаем системы предотвращения от проникновения, которые могут и обнаружить и отключить неучтенные [rogue] точки доступа, а также [ad hoc] клиентов.

Если развернуто решение 802.1X/EAP для беспроводной сети, оно может быть также использовано для защиты сетевых портов на проводной сети. Лучший способ предотвращения неучтенного доступа - это контроль портов на проводной стороне. 802.1X/EAP можно также использовать для аутентификации и авторизации доступа через проводные порты на коммутаторе уровня доступа. Неучченное устройство не может действовать в качестве беспроводного портала к сетевым ресурсам, если неучченное устройство включено в управляемый порт, который блокирует трафик более высокого уровня. Когда 802.1X/EAP используется для контроля портов на коммутаторе уровня доступа, настольные клиенты работают как клиенты [supplicants], запрашивающие доступ. Некоторые ТД производителей БЛВС также могут работать как клиенты [supplicants] и не пересыпать пользовательский трафик, до тех пор пока проверенная ТД не аутентифицирована. Следовательно, проводное решение 802.1X/EAP является прекрасным методом предотвращения неучтенного [rogue] доступа. Некоторые производители БЛВС начали поддерживать MACsec для контроля проводных портов. Стандарт IEEE 802.1AE Безопасность Контроля Доступа к Среде [Media Access Control Security], часто называется MACsec, определяет набор протоколов для обеспечения требований безопасности для защиты данных, передающихся по Ethernet ЛВС. В этом случае, любое новое устройство, включая ТД, должно быть аутентифицировано сетью, прежде чем ему будет дан доступ. Это хороший способ не только использования существующих ресурсов, но также обеспечения лучшей защиты для вашей проводной сети путем защиты от неучтенных ТД.



Множество предприятий не используют решение 802.1X/EAP для контроля проводных портов. Следовательно, система мониторинга БЛВС, называемая системой обнаружения беспроводного вторжения [wireless intrusion detection system (WIDS)], обычно рекомендуется для обнаружения потенциальных неучтенных устройств. Большинство производителей WIDS называют свои продукты системой предотвращения беспроводного вторжения [wireless intrusion prevention system (WIPS)]. Причина, по которой они так называют в том, что они также способны отражать атаки от неучтенных ТД [rogue AP] и неучтенных клиентов [rogue client].

## Пиринговые (peer-to-peer) атаки

Обычно не принимаемый во внимание риск - *пиринговая атака* или *атака при соединении типа равный-с-равным* [*peer-to-peer attack*]. Как вы знаете из ранних глав клиентская станция 802.11 может быть настроена как в режим работы инфраструктуры, так и в режим "на лету" [*ad hoc*]. При настройке в режим "на лету" [*ad hoc*], беспроводная сеть официально стандартом 802.11 называется как *независимый базовый состав сервиса* [*independent basic service set (IBSS)*], и все связи являются равный-с-равным [*peer-to-peer*] без необходимости в точке доступа. Так как IBSS по природе соединение типа равный-с-равным [*peer-to-peer*], любой пользователь, который может беспроводным способом подключиться к другому пользователю, может потенциально получить доступ к любому ресурсу, доступному на другом компьютере. Типовое использование сетей по запросу [*ad hoc networks*] - в обмене файлами на лету. Когда предоставляется общий доступ, файлы и другие ресурсы могут стать случайно видны всем.

Персональный межсетевой экран [*firewall*] часто используется для смягчения атак при подключении типа равный-с-равным [*peer-to-peer*]. Некоторые клиентские устройства могут также выключить эту функцию так, чтобы устройство подключалось только к определенным сетям, и не ассоциировалось с сетью равный-с-равным [*peer-to-peer*] без подтверждения.

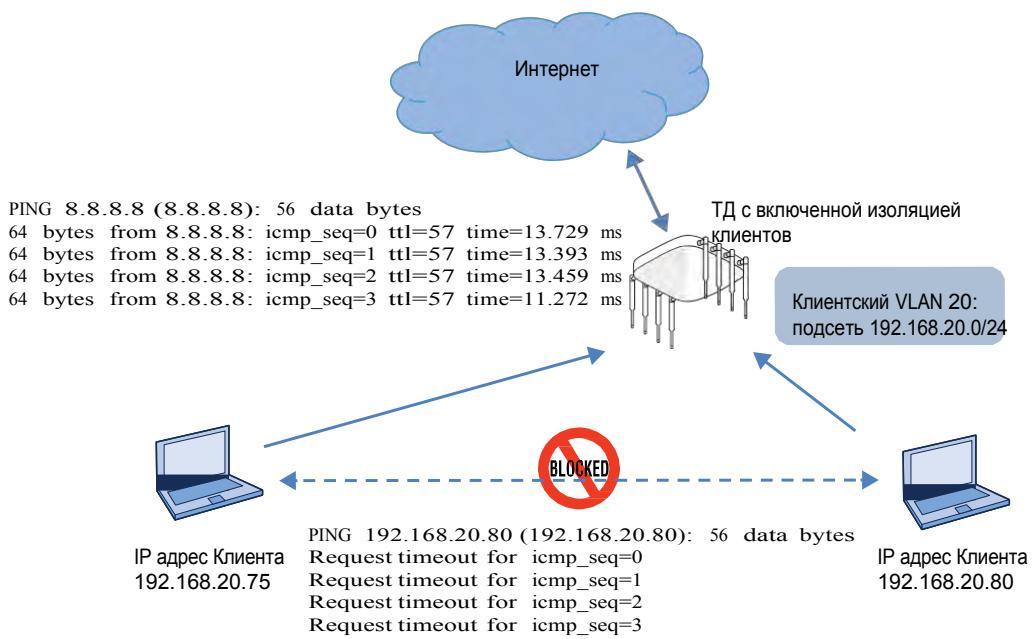
Пользователи ассоциированные с той же самой точкой доступа потенциально также уязвимы для пиринговых [*peer-to-peer*] атак как и IBSS пользователи. Надлежащая защита вашей беспроводной сети часто включает в себя защиту авторизованных пользователей друг от друга, так как взлом в компаниях часто осуществляется сотрудниками изнутри. Любые пользователи, ассоциированные с одной и той же ТД, и которые являются членами тогоже самого базового состава сервиса [*basic service set (BSS)*], и находятся в одном и том же VLANe, уязвимы для атак равный-с-равным [*peer-to-peer*], потому что они находятся в одних и техже доменах уровня 2 и уровня 3. В большинстве установок БЛВС Wi-Fi клиенты взаимодействуют только с устройствами в проводной сети, такими как сервер электронной почты или веб серверы, и взаимодействие клиент-клиент [*peer-to-peer*] не нужно. Следовательно, большинство производителей корпоративных ТД предоставляют некий собственный способ, предотвращающий пользователей от неосторожного предоставления общего доступа к файлам другим пользователям или транзитного (мостового) трафика между устройствами. Когда требуются соединения с другими беспроводными клиентами, трафик маршрутизируется через коммутатор Зого уровня или другое сетевое устройство прежде, чем попасть к желаемой станции назначения.

*Изолирование клиентов* [*Client isolation*] это функция, которая может быть часто включена на точках доступа или контроллерах БЛВС, для блокировки беспроводных клиентов от взаимодействия с другими беспроводными клиентами в одном и том же беспроводном VLANe. Изолирование клиентов, или другие различные термины, используемые для описания этой функции, обычно означают, что пакеты, прибывающие на беспроводной интерфейс ТД, не пересылаются обратно в беспроводной интерфейс другим клиентам. Это изолирует каждого пользователя на беспроводной сети, чтобы гарантировать, что беспроводная станция не может быть использована для получения доступа уровня 3 или выше к другой беспроводной станции. Функция изолирования клиентов обычно настраиваемый параметр для каждого SSID, связанного с уникальным VLAN. Как показано на Рисунке 16.3, с включенным изолированием клиентов, клиентские устройства не могут взаимодействовать напрямую с другими клиентскими устройствами на беспроводной сети.



Хотя изолирование клиентов – это наиболее широко употребительный термин, некоторые производители используют термин *блокировка клиент-клиент* [*peer-to-peer blocking*] или публичная безопасная пересылка пакетов [*public secure packet forwarding (PSPF)*]. Не все производители реализуют изолирование клиентов одинаковым способом. Некоторые производители БЛВС применяют изолирование клиентов только на паре SSID/VLAN на одной точке доступа, в то время как другие могут применить возможности блокировки между клиентами [*peer-blocking*] по нескольким ТД.

РИСУНОК 16.3 Изолирование клиентов



Некоторые приложения требуют связность клиент-клиент [peer-to-peer]. Многие телефоны с Голосом поверх Wi-Fi [Voice over Wi-Fi (VoWiFi) phones] предлагают функционал нажми-чтобы-говорить [push-to-talk], которые используют многоадресное вещание [multicasting]. Телефоны VoWiFi обычно отделены в отдельный беспроводной VLAN от других беспроводных клиентов с передачей данных. Изолирование клиентов не должно применяться в VoWiFi VLAN, если требуется многоадресное вещание [multicasting] для нажми-чтобы-говорить [push-to-talk], так как это может помешать этим устройствам работать надлежащим образом.

## Прослушивание

Как мы упоминали в этой книге, беспроводные сети 802.11 работают в полосах частот не требующих получения лицензии, и все передачи данных идут в открытом эфире. Доступ к беспроводным передачам доступен любому в пределах расстояния слышимости, а следовательно сильное шифрование обязательно. Беспроводную связь можно мониторить двумя способами прослушивания: обычное прослушивание [casual eavesdropping] и прослушивание со злым умыслом [malicious eavesdropping].

*Обычное прослушивание [Casual eavesdropping]*, иногда называемое *обнаружение БЛВС [WLAN discovery]*, выполняется простым использованием методов обмена кадрами 802.11, которые четко определены стандартом 802.11-2020. Программные утилиты, называемые как *инструменты по обнаружению БЛВС [WLAN discovery tools]*, существуют для целей по нахождению открытых сетей БЛВС. Как мы обсудили в Главе 9 "802.11 MAC", для того, чтобы клиентская станция 802.11 могла подключиться к точке доступа, он должна сначала обнаружить точку доступа. Станция обнаруживает точку доступа путем прослушивания ТД (пассивное сканирование)

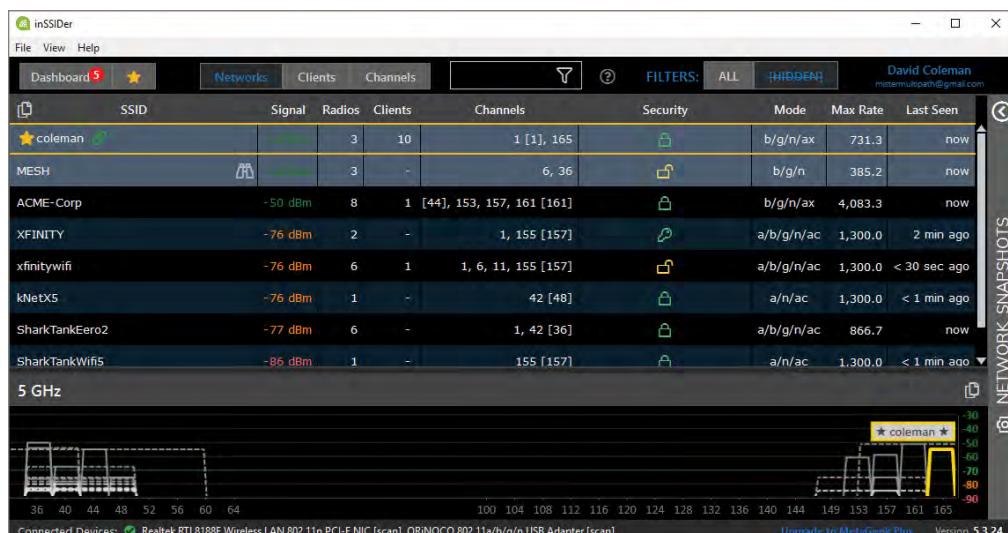
[(passive scanning)] или поиском ТД (активное сканирование) [(active scanning)]. В *пассивном сканировании [passive scanning]*, клиентская станция слушает кадры управления 802.11 - маяки [beacon], которые непрерывно посылаются точками доступа.

Обычное прослушивание может просто использовать любой клиентский радиомодуль 802.11 для прослушивания кадров управления 802.11-маяков и обнаружить информацию уровня 2 о БЛВС. Некоторая информация, находящаяся в кадрах маяках включает в себя идентификатор состава сервиса [service set identifier (SSID)], MAC адреса, поддерживаемые скорости передачи данных, и другие возможности базового состава сервиса [basic service set (BSS)]. Вся эта информация уровня 2 передается открытым текстом и может быть просмотрена любым радиомодулем 802.11.

В дополнение к пассивному сканированию ТД, клиентские станции могут сканировать их активно. В *активном сканировании [active scanning]* клиентская станция передает кадры управления, называемые зондирующими запросами [probe requests]. Точка доступа затем отвечает обратно *кадром ответа на зондирующий запрос* или *зондирующем ответом [probe response frame]*, который в основном содержит всю ту же самую информацию уровня 2, находящуюся в кадре -маяке. Зондирующий запрос [probe request] без информации о SSID называется *пустым зондирующим запросом [null probe request]*. Если отправлен направленный зондирующий запрос, все ТД, которые поддерживают этот конкретный SSID и услышавшие запрос, должны ответить путем отправки зондирующего ответа. Если же услышан пустой зондирующий запрос, то все ТД, независимо от их SSID, должны ответить зондирующими ответом [probe response].

Многие программные утилиты беспроводных клиентов инструктируют радиомодуль для передачи зондирующих запросов с пустыми полями SSID при активном сканировании при поиске ТД. Дополнительно, существует многочисленные бесплатные и коммерческие приложения-инструменты по обнаружению БЛВС. Инструменты обнаружения БЛВС отправляют пустые зондирующие запросы по всем не требующим лицензии каналам 802.11 в надежде получить кадры ответов на зондирующий запрос, содержащий информацию о беспроводной сети, такую как SSID, канал, шифрование, и т.д. Некоторые инструменты обнаружения БЛВС также могут использовать пассивные методы сканирования. Показанный на Рисунке 16.4, очень популярный инструмент обнаружения БЛВС на OC Windows - inSSIDer, который доступен с вебсайта [www.metageek.net](http://www.metageek.net).

#### РИСУНОК 16.4 MetaGeek inSSIDer



Обычное прослушивание может обнаружить сети 802.11 путем использования программных инструментов, которые рассылают пустые зондирующие запросы. Обычное прослушивание обычно считается безвредным и часто называется *вардрайвингом* [ *wardriving*, (в переводе - *военная езда*)]. Вардрайвинг - это строго действие по поиску беспроводных сетей, обычно при движении транспорта. Термин вардрайвинг [*wardriving*] был выведен от слова вардайлинг [*wardialing* (в переводе военный обзор)] из фильма 1983 года *Военные игры* [*WarGames*]. Вардайлинг [*wardialing*] был техникой применяемой хакерами, использующими компьютерные модемы для автоматического сканирования тысячи телефонных номеров в поиске других компьютеров, с которыми они могли бы быть соединены.

Вардрайвинг [*Wardriving*] теперь считается устаревшим термином и концепцией. В самые ранние дни Wi-Fi, вардрайвинг [*wardriving*] было хобби и спорт для техно-гиков и хакеров, ищущих БЛВСы. Соревнования по вардрайвингу [*wardriving*] проводились на хакерских съездах, чтобы посмотреть кто больше найдет БЛВСов.

В то время как спорт вардрайвинга затух, миллионы людей продолжают использовать инструменты обнаружения БЛВС, чтобы найти доступные Wi-Fi сети. Более современный термин будет "обнаружение БЛВС" ["*WLAN discovery*"] В ранние дни Wi-Fi изначальный программный инструмент обнаружения БЛВС был бесплатной программой с названием NetStumbler. Хотя он все еще доступен для бесплатной загрузки, NetStumbler не обновлялся многие годы. Однако, есть многое более новых инструментов по обнаружению БЛВС, которые работают на различных операционных системах. Рисунок 16.5 изображает инструмент обнаружения БЛВС на базе Android - WiFi Analyzer. Многочисленные инструменты обнаружения БЛВС доступны для мобильных Android устройств, но на текущий момент существует не много инструментов для мобильных iOS устройств из-за ограничений разработчиков применяемой компанией Apple.

**РИСУНОК 16.5** Инструмент обнаружения БЛВС WiFi Analyzer



По проекту, сама природа пассивного и активного сканирования 802.11 заключается в предоставлении идентификационной сетевой информации, которая доступна любому с радиомодулем 802.11. Поскольку это неотъемлемая и необходимая функция 802.11, то вардрайвинг [wardriving] не является преступлением. Законность использования чьей-то беспроводной сети без разрешения часто не ясна, но предупреждаем, что людей арестовывали и преследовали в судебном порядке в результате таких действий. Тревожное решение об использовании сетей, принадлежащих другим лицам, было принято в марте 2011 года. Гаагский суд постановил, что они больше не собираются рассматривать как криминальный поступок неавторизованное использование сетей, принадлежащих другим лицам, если лицо, использующее сеть без разрешения, использовало ее только для доступа в Интернет, даже если доступ был получен экстраординарными средствами. Постановление оставляет возможность для гражданского иска. У каждой нации есть свои законы описывающие такие действия.



Мы не поощляем и не поддерживаем попытки использования беспроводных сетей, для которых у вас нет разрешения для использования. Мы рекомендуем, чтобы вы подключались только к беспроводным сетям, к которым у вас есть разрешенный доступ.

### Какие инструменты нужны для обнаружения БЛВС?

Чтобы начать искать БЛВСы, вам нужны клиентская сетевая карта(NIC) 802.11 и приложение по обнаружению БЛВС [WLAN discovery]. Существуют многочисленные бесплатные и коммерческие инструменты обнаружения, включая inSSIDer для Windows, WiFi Explorer для Windows, Acrylic Wi-Fi для Windows, WiFi Explorer для macOS, и WiFi Analyzer для Android. Вы можете загрузить inSSIDer с [www.metageek.com](http://www.metageek.com), WiFi Pro или Lite с [www.helge-keck.com](http://www.helge-keck.com), Acrylic Wi-Fi Home или Professional с [www.acrylicwifi.com](http://www.acrylicwifi.com), WiFi Explorer или WiFi Explorer Pro с [www.intuitibits.com](http://www.intuitibits.com), и WiFi Analyzer с [bit.ly/WiFIAalyze](http://bit.ly/WiFIAalyze).

Устройства системы глобального позиционирования (GPS) совместно с инструментами обнаружения БЛВС могут быть использованы для внесения отметки координат долготы и широты сигнала от обнаруженной ТД. Файлы записи обнаружения БЛВС с GPS координатами могут быть загружены в большую базу данных с динамической привязкой в Интернете. Движок Географической Записи Беспроводных Сетей [Wireless Geographic Logging Engine (WIGLE)] поддерживает базу данных с возможностью поиска с более чем 675 миллионов Wi-Fi сетей. Зайдите на [www.wigle.net](http://www.wigle.net), и наберите ваш адрес, чтобы увидеть обнаружены ли уже какие-либо беспроводные точки доступа по соседству с вами.

В то время как обычное прослушивание [casual eavesdropping] считается безвредным, то прослушивание со злым умыслом [*malicious eavesdropping*], неразрешенное использование анализаторов протоколов 802.11 для записи беспроводной связи, обычно считается незаконным. В большинстве стран есть определенного вида законы о подслушивании, которые гласят что прослушивание телефонного разговора кого-нибудь еще является преступлением. Кроме того, в большинстве стран законы объявляют незаконным прослушивание любого вида электромагнитной связи, включая беспроводную передачу 802.11.

Приложение анализатор протоколов 802.11 позволяет администраторам беспроводных сетей записывать трафик 802.11 с целью анализа и решения проблем своих собственных беспроводных сетей. Анализатор протоколов – это пассивное устройство, которое работает в режиме радиомониторинга для записи любой передачи кадра 802.11 в пределах радиуса действия. Так как анализаторы протоколов перехватывают кадры 802.11 пассивно, то система предотвращения беспроводного вторжения [wireless intrusion prevention system (WIPS)] не может обнаружить злонамеренное прослушивание [malicious eavesdropping]. В доступе есть коммерческие анализаторы протоколов БЛВС, такие как Savvius Omnipeek, а так же и популярный бесплатный анализатор протоколов Wireshark ([www.wireshark.org](http://www.wireshark.org)).

Подразумевается, что анализатор протоколов БЛВС будет использоваться как диагностический инструмент. Однако, атакующий может использовать анализатор протоколов БЛВС в качестве злонамеренного прослушивающего устройства для мониторинга обмена кадров 802.11 без разрешения. Хотя вся информация уровня 2 всегда доступна, вся информация уровней 3-7 может быть видна, если не используется шифрование WPA2/WPA3. Любая связь открытым текстом, такая как электронная почта, FTP, и пароли Telnet могут быть перехвачены, если нет никакого шифрования. Более того, любая незашифрованная передача кадров может быть воссоздана на более высоких уровнях модели OSI. Сообщения электронной почты могут быть воссозданы и, следовательно, прочитаны подслушивающим. Также могут быть воссозданы веб страницы и мгновенные сообщения [instant messages]. Могут быть воссозданы пакеты VoIP и записаны в формате звукового файла WAV. Злонамеренное подслушивание в таком виде – абсолютно незаконно.

Из-за пассивной и неопределенной природы этой атаки, должно всегда применяться шифрование, чтобы обеспечить конфиденциальность данных. Шифрование – это лучшая защита от неавторизованного мониторинга БЛВС. Шифрование WPA2/WPA3 обеспечивает конфиденциальность данных для информации всех уровней 3-7.



Самые типовые цели атак злонамеренного прослушивания это хотспоты публичного доступа. Публичные хотспоты редко предлагают защиту и обычно передают данные без шифрования, делая пользователей хотспота первичными целями. В результате, в приказном порядке должны быть внедрены решения защищенной VPN для всех мобильных пользователей, которые подключаются за пределами сети вашей компании.

## Взлом Шифрования

Конфиденциальность Эквивалентная Проводной [Wired Equivalent Privacy (WEP)] - это устаревший метод шифрования в 802.11, который был скомпрометирован много лет назад. Инструменты по взлому WEP [WEP-cracking tools] свободно доступны в Интернете и могут взломать шифрование WEP менее чем за 5 минут. Существует несколько методов, используемых для взлома шифрования WEP. Однако, атакующему обычно нужно только перехватить несколько сотен тысяч зашифрованных пакетов анализатором протоколов, а затем пропустить перехваченные данные через программное обеспечение по взлому WEP, как показано на Рисунке 16.6. Далее программа утилита обычно может вывести секретный 40-битный или 104-битный ключ за секунды. После того, как секретный ключ раскрыт, атакующий может расшифровать любой или весь зашифрованный трафик. Другими словами, атакующий может даже прослушивать зашифрованную с помощью WEP сеть. Так как атакующий может расшифровать трафик, то он может воссоздать данные и прочитать их, если больше не было никакого шифрования.

**РИСУНОК 16.6 Утилита взлома WEP**

```
* Got 286716! unique IVs | fudge factor = 2
* Elapsed time [00:00:03] | tried 1 keys at 20 k/m

KB    depth   votes
0     0/   1   DA( 60) 70( 23) 55( 15) A2(  5) CD(  5) 3E(  4)
1     0/   2   BD( 57) 2A( 32) 29( 22) 1D( 13) F9( 13) 9F( 12)
2     0/   1   8C( 51) 67( 23) 48( 15) DD( 15) D6( 13) FA( 12)
3     0/   3   1D( 30) A5( 17) 07( 15) 7B( 12) 4B( 10) 63( 10)
4     0/   1   43( 66) B1( 15) D2(  6) 1A(  5) 20(  5) 21(  5)
5     0/   5   92( 27) 23( 25) 02( 18) 2F( 17) C1( 16) 36( 12)
6     0/   1   C6( 51) 54( 17) 50( 15) 66( 15) 01( 13) 4A( 13)
7     0/   2   84( 29) C0( 17) EE( 13) 80( 12) 49( 11) F6( 11)
8     0/   1   81(1808) 09( 119) 99( 116) 32( 75) 49( 75) 9D( 65)
9     0/   1   C4(1947) E1( 125) FC( 123) BD( 105) 8C( 98) 2F( 85)
10    0/   1   8A( 580) 41( 120) 18(  93) ED(  85) B0(  65) 97(  60)
11    0/   1   08(  97) FF(  29) 5D( 20) 1E( 17) 18( 15) 5E( 15)
12    0/   1   1B( 145) DD( 21) 46( 20) 1C( 15) 76( 15) 07( 13)

KEY FOUND! [ DABD8C1D4392C68481C48A081B ]
```

**Атака с переустановкой ключа [KRACK Attack]**

В октябре 2017 года бельгийские исследователи Мэти Ванхуф [Mathy Vanhoef] и Франк Писсенс [Frank Piessens] Лёвенского Университета опубликовали подробности атаки с переустановкой ключа (KRACK). Эта повторяемая атака нацелена на 4x-Стороннее Рукопожатие [4-Way Handshake], используемое для установки динамических ключей шифрования в протоколе WPA2.

Уязвимость KRACK получила широкое освещение в прессе из-за потенциальной возможности компрометации ключей шифрования для многих существующих Wi-Fi устройств. Объяснение того, как работает атака, находится за пределами этой книги, но вы можете найти больше информации на [www.krackattacks.com](http://www.krackattacks.com).

Хорошая новость, что уязвимость KRACK можно легко исправить путем установки исправлений прошивки [firmware patches]. Все основные производители БЛВС быстро отреагировали в 2017 году и выпустили обновления ПО [firmware updates]. Но большой вопрос в обновлении ПО клиентских устройств. Хотя уязвимость залатали во всех основных операционных системах клиентских устройств, у многих устаревших клиентов может не быть доступного обновления ПО.

**Уязвимость Kr00k**

На конференции по безопасности RSA 2020 в Сан Франциско исследователи из словацкой антивирусной компании ESET представили подробности новой уязвимости связи. Kr00k - это уязвимость в чипах радиомодулей Broadcom и Cypress, которая позволяет неавторизованную дешифровку некоторого зашифрованного WPA2 трафика. Эта уязвимость может быть использована во время процесса MAC уровня, называемого диассоциацией [disassociation], которая представляет собой очень короткое окно времени, когда клиент и ТД завершают Wi-Fi связь между двумя устройствами. Во время процесса диассоциации [disassociation] клиента, ключи шифрования немедленно удаляются и заменяются на ключ, состоящий из всех нулей. Оборудование не принимает далее Wi-Fi трафик для передачи, но трафик, который уже в очереди на передачу, не сбрасывается так быстро. Например, кадры уже забуферизированы в очереди на передачу в оборудовании будут зашифрованы ключом с нулями и затем переданы.

Атакующий, мониторящий эту передачу может расшифровать несколько кадров. Другими словами, в худшем случае только несколько кадров будет дешифровано, так что риск раскрытия како-либо критичной информации минимален. Однако, плохие атакующие [black-hat attacker] могут получить доступ к нескольким килобайтам чувствительным данным, особенно, если атакующий повторно инициирует процесс диассоциации [disassociation]. Хотя уязвимость исправлена на всех основных операционных системах клиентских устройств, у многих устаревших клиентов может не быть доступного обновления ПО.

## Аутентификационные атаки

Как вы уже знаете, разрешение или авторизация к сетевым ресурсам может быть получена или с помощью решения с аутентификацией 802.1X/EAP или с использованием аутентификации PSK. Стандарт 802.11-2020 не определяет какой тип метода аутентификации EAP использовать, и все разновидности EAP созданы неодинаковыми. Некоторые типы аутентификации EAP более защищены, чем другие. *Облегченный Расширенный Протокол Аутентификации [Lightweight Extensible Authentication Protocol (LEAP)]*, когда-то одно из наиболее часто используемых решений 802.1X/EAP, является уязвимым к оффлайн атакам перебора по словарю. Ответ с захэшированным паролем во время процесса аутентификации LEAP является легко взламываемым.

Атакующему нужно всего лишь записать обмен кадрами во время пользовательской LEAP аутентификации и пропустить файл с записью через оффлайн инструмент атаки перебора по словарю, как показано на Рисунке 16.7. Пароль может быть вычислен за секунды. Имя пользователя также видно открытым текстом во время процесса аутентификации LEAP. После того как атакующие получают имя пользователя [username] и пароль [password], они могут выдавать себя за пользователя путем аутентификации в БЛВС, и затем получить доступ к любым сетевым ресурсам, которые доступны этому пользователю. Более сильные аутентификационные протоколы EAP, которые туннелируют аутентификационный трафик, не подвержены оффлайн атакам перебора по словарю.

РИСУНОК 16.7 Оффлайн атака перебора по словарю

The screenshot shows a terminal window titled '<Finished> - /root/asleap - Konsole'. The window displays several sections of captured LEAP authentication information:

- Captured LEAP auth success:**

```
0025 0215 0025 1101 0018 b1b6 6613 94b9 %.%.%.f...
a076 15e7 07b3 5234 3033 0b55 4b30 f276 .v....R403.UK0.v
12a4 7465 7374 32 .. david
```
- Captured LEAP exchange information:**

```
username: david
challenge: 373931a2d1888e58
response: b1b6661394b9a07615e707b3523430330b554b30f27612a4
Attempting to recover last 2 of hash.
hash bytes: f2d8
Starting dictionary lookups.
NT hash: f70da7fad38a37d803d9f737a286f2d8
password: 123abc123abc
```
- Reached EOF on pcapfile.**

Самый большой риск любой аутентификационной атаки в том, что все сетевые ресурсы становятся уязвимыми, если аутентификационные учетные данные скомпрометированы. Риски аутентификационной атаки аналогичны неучтенным [rogue] точкам доступа. Если авторизованный портал БЛВС может быть скомпрометирован и могут быть получены аутентификационные учетные данные, то сетевые ресурсы являются раскрытыми. Из-за этих серьезных рисков, корпоративная инфраструктура БЛВС должны быть защищена надлежащим образом решением 802.1X/EAP, которое использует RADIUS сервер и туннелированные аутентификационные EAP протоколы, обсуждаемые в Главе 17.

Так как у большинства домашних пользователей нет RADIUS сервера, они обычно используют более слабые методы аутентификации WPA/WPA2-Personal. WPA/WPA2-Personal, использующий пароль [passphrase] (иногда называется как заранее известный общий ключ [preshared key], или PSK), является слабым аутентификационным методом, который уязвим для онлайновых усиленных атак перебора по словарю [*brute-force dictionary attack*]. Общие ключи [Shared keys] или пароли [passphrases] также легко получить с помощью методов социальной инженерии. *Социальная инженерия [Social engineering]* - это действие по манипуляции людьми для выполнения действий или разглашения конфиденциальной информации. Атакующий, который получает пароль, может ассоциироваться с точкой доступа WPA/WPA2 и получить доступ к сетевым ресурсам. Чтобы помочь нивелировать онлайн усиленные атаки перебора по словарю, IEEE и Wi-Fi Альянс рекомендуют использовать очень сложный пароль в 20 или более знаков всегда, когда развернутое решение WPA/WPA2-Personal. Длина пароля WPA/WPA2 может быть в диапазоне от 8 до 63 знаков. Самый большой риск при любой аутентификационной атаке в том, что все сетевые ресурсы могут стать уязвимыми, если аутентификационные учетные данные скомпрометированы. В Главе 17 вы узнаете, что WPA3-Personal кладет конец усиленным атакам перебора по словарю с помощью использования аутентификационного протокола с названием *Одновременная Аутентификация Равных [Simultaneous Authentication of Equals (SAE)]*. Однако, статические пароли остаются уязвимыми для атак социальной инженерии.

Еще хуже то, что после получения пароля, хакер может расшифровать динамически создаваемый ключ шифрования TKIP/ARC4 или CCMP/AES. Пароль используется для получения *парного мастер ключа [pairwise master key (PMK)]*, который используется в *4x-Стороннем Рукопожатии [4-Way Handshake]* для создания финальных динамических ключей шифрования. Если у хакера есть пароль и перехваченное 4x-Стороннее Рукопожатие, то они могут воссоздать динамические ключи шифрования и расшифровать трафик. WPA/WPA2-Personal не считается решением с сильной защитой для предприятий, атакующий может не только получить доступ к сетевым ресурсам, но также может расшифровать трафик. Из-за этих рисков решение аутентификации со статичным PSK не должны применяться на предприятиях. В случае, когда нет сервера AAA или клиентские устройства на поддерживают 802.1X/EAP, рекомендуются проприетарные решения с аутентификацией PSK, применяющие уникальные PSK. Несколько производителей корпоративных БЛВС предлагают проприетарные PSK решения, которые предоставляют возможность предоставления уникального PSK для каждого пользователя.




---

Вы узнаете больше о 4x Стороннем Рукопожатии [4-Way Handshake] и генерации динамических ключей шифрования в Главе 17 "Архитектура Сетевой Безопасности 802.11"

## Подмена MAC

У всех радиомодулей 802.11 есть физический адрес, который называется MAC адрес [MAC address]. Этот адрес состоит из 12 шестнадцатеричных чисел, которые видны открытым текстом в заголовке 2ого уровня кадров 802.11. Производители Wi-Fi часто предоставляют возможности фильтрация по MAC на своих ТД. Обычно, MAC фильтры настраиваются, чтобы применить ограничения, которые разрешают проходить трафику только от определенных клиентских станций. Эти ограничение основаны на уникальности их MAC адресов. Всем другим клиентским станциям, чьи MAC адреса находятся не в разрешенном списке, не смогут передать трафик через виртуальный порт точки доступа в среду распределительной системы [distribution system]. Фильтрация по MAC часто используется в качестве механизма защиты для устаревших клиентских устройств, таких как мобильные ручные сканеры, которые не поддерживают сильную аутентификацию и методы шифрования.

К сожалению, MAC адреса могут быть подменены [spoofed], или подделаны, и любой непрофессиональных хакер может просто пройти любой MAC фильтр путем подмены на адрес разрешенной клиентской станции.

Из-за возможности подмены [spoofing] и из-за всего объема административной работы, требующейся для настройки MAC фильтров, фильтрация по MAC не считается надежным средством безопасности для беспроводных корпоративных сетей, и может применяться только, если более сильная защита не доступна, или использоваться вместе с какой-либо более сильной формой защиты как часть многоуровневого плана безопасности.

## Использование уязвимостей интерфейса управления

Одна из главных целей атакующих - это получение доступа к административным учетным данным или корневым привилегиям [root privilege]. Заполучив этот доступ, они могут запустить несколько атак против сетей и индивидуальных устройств. На проводной сети эти атаки запускаются против межсетевых экранов, серверов, и инфраструктурных устройств. В беспроводной атаке, сначала запускаются против точек доступа или контроллеров БЛВС, а впоследствии против тех же самых целей, что и в проводных атаках. Оборудование беспроводной инфраструктуры, такое как точки доступа и контроллеры БЛВС, могут управляться администраторами через разные интерфейсы, почти также как управляется оборудование проводной инфраструктуры. Устройства обычно могут быть доступны по веб интерфейсу, интерфейсу командной строки, последовательному порту, консольному соединению, и /или по Простому Протоколу Сетевого Управления [Simple Network Management Protocol (SNMP)]. Эти интерфейсы должны быть защищены в приказном порядке. Интерфейсы, которые не используются, должны быть выключены. Должны всегда использоваться сложные пароли, и функции шифрованных входов[login] с использованием SSH2 (Secure Shell) или Защищенного Протокола Передачи Гипертекста [Hypertext Transfer Protocol Secure (HTTPS)].

Списки всех заводских настроек всех точек доступа основных производителей есть в Интернете, и они часто используются для взлома защиты хакерами. Не является не обычным для атакующих использовать дыры в безопасности, оставленные в интерфейсах управления, чтобы перенастроить ТД. Законные пользователи и администраторы могут однажды обнаружить, что они заблокированы на своем собственном Wi-Fi оборудовании. После получения доступа через интерфейс управления, атакующий может даже суметь инициировать обновление ПО [firmware] беспроводного оборудования, и пока происходит обновление, выключить питание оборудования. Эта атака может с высокой вероятностью сделать оборудование бесполезным, требующего вернуть его производителю для восстановления.

Политика часто предписывает, чтобы все инфраструктурные устройства БЛВС настраивались только с проводной стороны сети. Если администратор попытается настроить оборудование БЛВС, при этом подключенным беспроводным способом, то администратор может потерять соединение из-за сделанных изменений в конфигурации. Некоторые производители БЛВС предлагают возможности безопасного беспроводного консольного подключения для решения проблем и настройки.

## Беспроводной угон [Hijacking]

Атака, которая часто вызывает массу статей в прессе, это беспроводной угон [*wireless hijacking*], также называется как *атака “злой двойник”* [*evil twin attack*]. Атакующий настраивает программу точки доступа на ноутбуке, фактически превращая клиентский Wi-Fi радиомодуль в точку доступа. У некоторых небольших Wi-Fi USB устройств также есть возможность работать как ТД. Программа точки доступа на ноутбуке атакующего настраивается с тем же самым SSID, который используется публично доступным хотспотом. Теперь точка доступа атакующего работает как ТД “Злой Двойник”, но передающая на другом канале. Атакующий затем посыпает поддельные кадры диассоциации и деаутентификации, форсируя пользователей, ассоциированных с точкой доступа хотспота, переключаться на точку доступа “злого двойника”. В этом месте, атакующий фактически угоняет беспроводных клиентов на 2ом уровне у исходной ТД. Хотя кадры деаутентификации обычно используются как один из способов начала атаки по угону [*hijacking attack*], также может быть использована радиоглушилка [*RF jammer*], чтобы форсировать всех клиентов переключиться на ТД “злой двойник”.

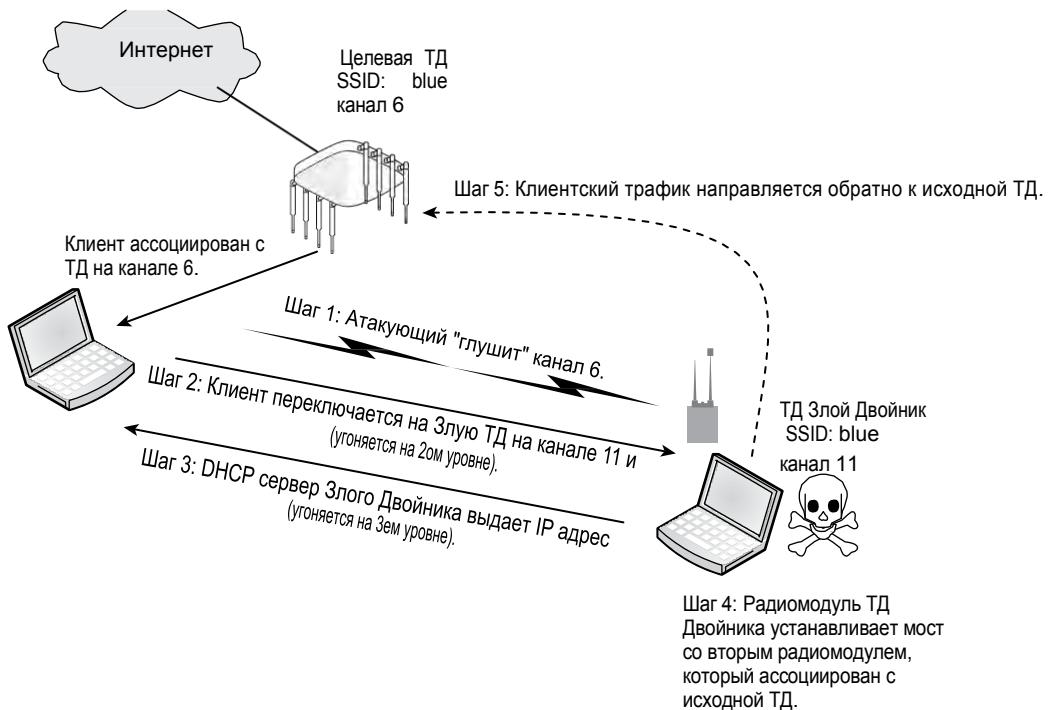
Злой двойник обычно настраивается с сервером Протокола Динамической Настройки Хостов [*Dynamic Host Configuration Protocol (DHCP)*], готовым выдавать IP адреса клиентам. В этой точке атакующий угоняет [*hijacked*] пользователей на Зем уровне, и теперь имеет частную беспроводную сеть , и может теперь проводить атаки равный-сравненным [*peer-to-peer*] на любого из угнанных клиентов [*hijacked clients*]. Пользовательский компьютер может во время процесса подключения к злому двойнику стать жертвой DHCP атаки, атака, которая использует процесс DHCP, чтобы загрузить набор утилит для удаленного управления [*root kits*] или другого вредоносного ПО на компьютер жертвы в дополнение к выдаче ожидаемого IP адреса.

Атакующий также может использовать вторую беспроводную сетевую карту (NIC), чтобы произвести, так называемую, *атаку человек-по середине* [*man-in-the-middle attack*], как показано на Рисунке 16.8. Второй радиомодуль БЛВС ассоциирован с исходной точкой доступа как клиент. В операционных системах, сетевые интерфейсы можно объединить в мост, для обеспечения маршрутизации. Атакующий объединяет в мост свою вторую беспроводную карту (NIC) с радиомодулем Wi-Fi, который используется как точка доступа - злой двойник. После того, как атакующий угоняет пользователей с исходной ТД, то трафики перемаршрутизируется с ТД злой двойник на второй Wi-Fi радиомодуль, прямо обратно к исходной ТД, с которой пользователи только что были угнаны. В результате, пользователи остаются угнанными; однако, у них остается маршрут обратно через шлюз к своей исходной сети, так что они никогда не узнают, что они были угнаны. Следовательно, атакующий может сидеть по середине и проводить атаки равный-с-равненным [*peer-to-peer*] бесконечно, пока остается полностью незамеченым.

Эти атаки могут принять другую форму, так называемую, *фишинговая Wi-Fi атака* [*Wi-Fi phishing attack*]. У атакующего также может быть программное обеспечение веб сервера и программное обеспечение перехватывающего портала [*captive portal*]. После того как пользователи были угнаны на точку доступа - злого двойника, они могут быть перенаправлены на веб страничку входа [*login web page*],

которая может выглядеть как страница входа хотспота. Тогда поддельная страничка атакующего может запросить номер кредитной карты у угоннного пользователя. Фишинговые атаки распространены в Интернете, а теперь появляются и на вашем локальном хотспоте.

**РИСУНОК 16.8** Атака беспроводной «угон»/человек-по-середине



Единственный способ предотвратить угон [hijacking], человека-по-середине [man-in-the-middle] или фишинговые Wi-Fi атаки - это использовать решение с взаимной аутентификацией. Решения с взаимной аутентификацией не только подтверждают пользователя, подключающегося к сети, но они также подтверждают сеть, к которой подключается пользователь. Решение аутентификации 802.1X/EAP требует, чтобы обмен взаимными аутентификационными учетными данными был произведен до того, как пользователь может быть авторизован. Пользователь не сможет получить IP адрес, пока не авторизован; следовательно, пользователи не смогут быть угонаны.

## Атаки Отказа-в-Обслуживании

Атака на беспроводные сети, которая кажется получает меньше всего внимания – это атака отказа в обслуживании [*denial-of-service (DoS)*]. С соответствующими инструментами любой со злым умыслом может временно выключить Wi-Fi сеть, препятствуя законным пользователям получать доступ к сетевым ресурсам.

Хорошая новость, что существуют системы мониторинга, которые могут обнаружить и идентифицировать DoS атаки мгновенно. Плохая новость в том, что обычно ничего нельзя сделать, чтобы предотвратить DoS атаки, кроме как локализовать и устраниить источник атаки.

DoS атаки могут происходить на уровне 1 или на уровне 2 модели OSI. Атаки уровня 1 называются *атаками постановки радиопомех* [*RF jamming attacks*]. Два самых распространенных типа атак постановки радиопомех – это преднамеренная постановка помех [*intentional jamming*] и непреднамеренная постановка помех [*unintentional jamming*]:

**Преднамеренная постановка помех [Intentional Jamming]** Атаки преднамеренной или умышленной постановки помех происходят, когда атакующий использует своего рода генератор сигналов, чтобы вызвать интерференцию в нелицензируемом частотном пространстве. Существуют и узкополосные и широкополосные постановщики помех [*jammers*], которые будут инвертировать с передачами 802.11, или вызывая повреждение всех данных, или заставляя радиомодули 802.11 постоянно откладывать передачу при проведении *оценки чистоты каналы* [*clear channel assessment (CCA)*].

**Непреднамеренная постановка помех [Unintentional Jamming]** В то время как преднамеренная постановка помех является злонамеренной, непреднамеренная постановка помех является более обычной и распространенной. Непреднамеренная интерференция от микроволновых печей, беспроводных телефонов, и других устройств также может вызвать отказ в обслуживании [*denial of service*]. Хотя непреднамеренная постановка помех не обязательно является атакой, она может нанести столько же вреда, как и атака с преднамеренной постановкой помех.

Лучший инструмент по обнаружению любого типа интерференции на уровне 1 как преднамеренной, так и не преднамеренной, это анализатор спектра. Хорошим примером автономного анализатора спектра является USB анализатор спектра Wi-Spy, которые доступен на [www.metageek.com](http://www.metageek.com).

Более распространенные типы атак отказа-в-обслуживании, которые исходят от хакреов являются атаками DoS на 2ом уровне. Существует широкое разнообразие атак DoS 2ого уровня, которые являются результатом манипуляции с кадрами 802.11. Наиболее типовые включают подмену [*spoofing*] кадров диассоциации [*disassociation*] или деаутентификации [*deauthentication*]. Атакующий может отредактировать заголовок 802.11 и подменить MAC адрес точки доступа или клиента как в поле адрес передатчика [*transmitter address (TA)*], так и в поле адрес приемника [*receiver address (RA)*]. Атакующий затем непрерывно повторно передает подмениенный кадр деаутентификации. Станция, которая получает подмениенный кадр деаутентификации, думает, что подмениенный кадр пришел от законной станции и отключается на уровне 2.

Существует намного больше типов DoS атак на уровне 2, включая потоки запросов на ассоциацию [*association floods*], потоки запросов на аутентификацию [*authentication floods*], потоки запросов PS-Poll [*PS-Poll floods*], и атака на виртуальную несущую. К счастью, любая хорошая система обнаружения беспроводного вторжения сможет мгновенно предупредить администратора о DoS атаке 2ого уровня. Поправка 802.11w-2009 определяет механизмы защиты кадров управления [*management frame protection (MFP)*] для предотвращения подмены определенных типов кадров управления 802.11. Эти кадры 802.11w называются как *надежные кадры управления* [*robust management frames*]. Надежные кадры управления могут быть защищены сервисом защиты кадров управления и включают диассоциацию, деаутентификацию, и надежные кадры

действия. Кадры действия используются, чтобы запросить станцию выполнить действие от имени другой станции, а не все кадры действия являются надежными.

Стоит отметить, что поправка 802.11w не кладет конец всем DoS атакам 2ого уровня. Многочисленные DoS атаки 2ого уровня не могут быть предотвращены. В прошлом, механизмы 802.11w MFP не поддерживались широко с клиентской стороны, потому что поддержка MFP была опциональной. Однако, производители корпоративных БЛВС применяли механизмы 802.11w на точках доступа; следовательно, некоторые из наиболее типовых DoS атак уровня 2 могут быть предотвращены, если клиенты поддерживают 802.11w. С 2019 года Wi-Fi Альянс обязывает поддерживать защиту кадров управления для всех радиомодулей сертифицированных для WPA3 и для всех сертифицированных радиомодулей Wi-Fi 6 (802.11ax).

Анализатор спектра - это ваш лучший инструмент для обнаружения DoS атак уровня 1, а анализатор протоколов или беспроводная IDS - это ваш лучший инструмент по обнаружению DoS атак 2ого уровня. Лучший способ предотвратить атаку отказа-в обслуживании любого типа - это физическая безопасность. Авторы этой книги рекомендуют сторожевых собак и забор из колючей проволоки. Если это не вариант, то решения нескольких производителей предоставляют обнаружение вторжений на уровне 1 и 2.

### Где Можно Узнать Больше Об Оценке Рисков Безопасности БЛВС?

Эта глава охватывает основы атак на безопасность Wi-Fi и мониторинг вторжения. Хотя написано много книг о взломе беспроводных сетей, хорошее начало - это *CWSP Сертифицированный Профессионал Беспроводной Безопасности Официальное Учебное Руководство: Экзамен CWSP-205 (Sybex, 2016) [CWSP Certified Wireless Security Professional Official Study Guide: Exam CWSP-205 (Sybex, 2016)]*. Также доступно много инструментов по аудиту безопасности БЛВС для проверки на возможность проникновения в Wi-Fi.

Один из наиболее популярных инструментов тестирования Wi-Fi на проникновение - это Wi-Fi Pineapple. Wi-Fi Pineapple - это инструмент аудита БЛВС от Hak5, который использует специальное оборудование и ПО с веб интерфейсом. Больше информации о Wi-Fi Pineapple находится на [www.wifipineapple.com](http://www.wifipineapple.com).

Большинство эффективных инструментов аудита работают на Linux платформах, многие из которых доступны с загрузочных CD, таких как Kali Linux. Kali Linux, который имеет 600+ инструментов, это дистрибутив на основе Debian с коллекцией инструментов по безопасности и следственным мероприятиям. Kali Linux можно загрузить с [www.kali.org](http://www.kali.org).

## Атаки на оборудование конкретного производителя

Хакеры часто находят дыры в коде прошивок, используемых определенными производителями точек доступа БЛВС и контроллеров БЛВС. Новые уязвимости и атаки БЛВС обнаруживаются на регулярной основе, включая атаки на определенного производителя. Многие из этих специфичных для производителя эксплойтов [exploit] являются формой атаки на переполнение буфера. Когда атака на оборудование определенного производителя стала известна, то производитель обычно выпускает исправление прошивки в достаточно короткий срок. Если возможность взлома [exploit] обнаружена, то пострадавший производитель БЛВС выпускает рекомендации по защите о том, как избежать этого эксплойта. В большинстве случаев производитель БЛВС быстро выпускает исправление [patch], который может исправить проблему. Лучший способ избегания этих атак - это быть в информированным службой поддержки производителя вашей БЛВС и поддержкой самого свежего и полностью поддерживаемого ПО [firmware] на вашей инфраструктуре БЛВС. Как и у большинства инфраструктурного сетевого оборудования, ПО [firmware], работающее на контроллере БЛВС или ТД, будет иметь свой жизненный цикл. Перед обновлением администратор всегда должен проверять влияние на сервис последней версии ПО [firmware]. Однако, к обновлениям безопасности следует всегда относиться серьезно.

## Социальная инженерия

Хакеры не взламывают большинство проводных и беспроводных сетей с использованием программ и инструментов. Большинство взломов в компьютерной безопасности происходит из-за атак социальной инженерии. *Социальная инженерия [Social engineering]* - это метод, используемый для манипуляции людьми для разглашения ими конфиденциальной информации, такой как компьютерные пароли. Лучшая защита против атак социальной инженерии - это строгое следование политикам для предотвращения раскрытия конфиденциальной информации.

Любая информация, которая является статичной, чрезвычайно восприимчива к атакам социальной инженерии. Шифрование WEP использует статический ключ, а WPA/WPA2/WPA3-Personal требует использование статичного PSK или пароля.

## Мониторинг Вторжения

Когда люди думают о беспроводных сетях, они склонны думать в терминах доступа, а не в терминах атак или вторжений. Однако, становится все более необходимым постоянно мониторить многие типы атак на БЛВС, из-за их потенциального вреда, который они могут причинить. Предприятия всех размеров устанавливают беспроводные сети 802.11 для мобильности и доступа. На многих из этих сетей работает *система обнаружения беспроводного вторжения [wireless intrusion detection system (WIDS)]*, чтобы отслеживать атаки. Мониторинг беспроводного вторжения развивался с его создания. Сегодня у большинства систем есть методы по предотвращению или уменьшению нескольких хорошо известных атак. Следовательно, большинство производителей БЛВС называют свои решения как *система предотвращения беспроводного вторжения [wireless intrusion prevention system (WIPS)]*. В этой книге, мы будем использовать термин - система предотвращения беспроводного вторжения [wireless intrusion prevention system (WIPS)].

Решения распределенного мониторинга [distributed monitoring solutions] также могут иметь функционал по предотвращению вторжений, включая борьбу с неучтенными [rogue] ТД и клиентами. Использование распределенного мониторинга БЛВС и предотвращение неучтенных включений уменьшает время и затраты, требующиеся для поддержания хорошего состояния и безопасности беспроводной сети.

## Система предотвращения беспроводного проникновения (WIPS)

В сегодняшнем мире, система предотвращения беспроводного вторжения (WIPS) может быть необходима даже, если на объекте нет авторизованной Wi-Fi сети 802.11.

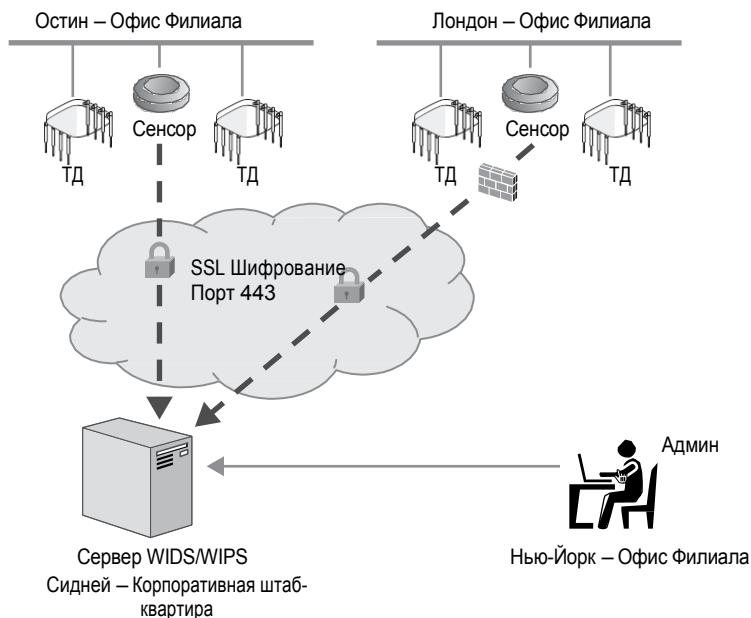
Беспроводная технология может быть технологией проникновения, и если порты данных на предприятии не контролируются, то любой (включая сотрудников) может установить неучщенную точку доступа [rogue access point]. Из-за этого риска многие компании—такие как банки, другие финансовые институты, и больницы—выбирают установку WIPS еще до развертывания Wi-Fi сети для доступа сотрудников. После того как сеть 802.11 установлена для доступа, становится почти строго обязательным также иметь WIPS из-за других многочисленных атак на Wi-Fi, таких как: DoS, угон БЛВС [hijacking], и т.д.

Обычная WIPS - это клиент-серверная модель, которая состоит из двух следующих компонентов::

**Сервер WIPS [WIPS Server]** Сервер WIPS - это программный сервер или аппаратный сервер, действующий в качестве центральной точки мониторинга безопасности и сбора данных производительности. Сервер использует анализ сигнатур, анализ поведения, анализ протоколов, и анализ радиоспектра, чтобы обнаружить потенциальные угрозы. Анализ сигнатур проверяет на соответствие моделям, связанным с распространенными атаками БЛВС. Анализ поведения следит за аномалиями 802.11. Анализ протоколов проверяет информацию MAC уровня из кадров 802.11. Анализ протоколов может также проверять информацию уровней 3-7 кадров данных 802.11, которая не зашифрована. Анализ спектра мониторит радиостатистику, такую как сила сигнала и отношение сигнал-шум (SNR). Анализ производительности может быть использован для измерения параметров состояния БЛВС, таких как емкость и покрытие.

**Сенсоры [Sensors]** Аппаратные или программные сенсоры могут быть размещены стратегически, чтобы слушать и записывать всю связь 802.11. Сенсоры - это глаза и уши системы мониторинга WIPS. Сенсоры используют радиомодули 802.11, чтобы собирать информацию, используемую для защиты и анализа трафика БЛВС. Рисунок 16.9 изображает клиент-серверную модель, используемую большинством систем предотвращения беспроводного вторжения.

**РИСУНОК 16.9** Система предотвращения беспроводного вторжения (WIPS)



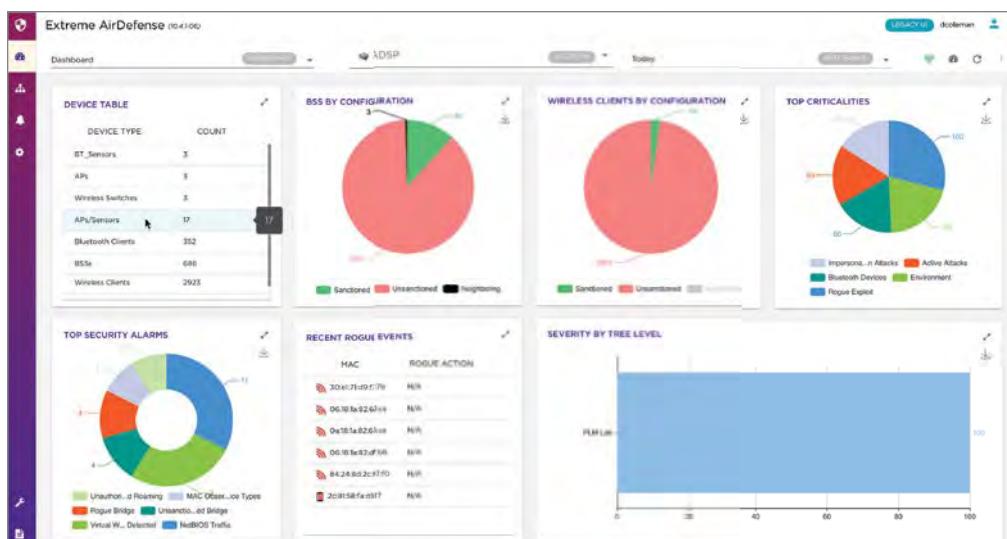
Сенсоры это в основном радиоустройства, которые постоянно находятся в режиме прослушивания как пассивные устройства. Сенсорные устройства обычно имеют аппаратную основу и похожи на точки доступа. У сенсоров есть некоторый интеллект, но одни должны взаимодействовать с центральным сервером WIPS. Центральный сервер собирает данные буквально от тысячи сенсоров из множества удаленных мест, и таким образом соответствует требованиям масштабируемости больших корпораций.

Отдельные сенсоры не предоставляют доступ клиентам БЛВС, потому что они настроены только на режим прослушивания. Сенсоры постоянно сканируют все каналы в полосе ISM 2,4 ГГц, а также все каналы в полосах U-NII 5 ГГц.

В редких случаях, сенсоры могут быть настроены на прослушивание только одного канала или выбранную группу каналов. Точки доступа также могут быть использованы как сенсоры работающие по определенному времени. ТД может использовать внеканальный [off-channel] метод сканирования, чтобы мониторить другие каналы, при этом продолжая проводить большую часть времени на домашнем канале ТД, для обеспечения доступа клиентам.

Многие ТД используют программно-определенный радиомодуль [*software-defined radio (SDR)*], у которого есть возможность работать или как приемо-передатчик в 2,4 ГГц или как приемопередатчик 5 ГГц, но он не может передавать на обоих частотных полосах одновременно. Однако, если SDR использует двух-диапазонный чипсет, то SDR может быть преобразован в постоянно работающий сенсор, который может слушать и полосу частот 2,4 ГГц и полосу частот 5 ГГц. Многие производители БЛВС теперь предлагают ТД с третьим радиомодулем, который работает как постоянный [full time] сенсор только в режиме прослушивания. Как показано на Рисунке 16.10, администратор БЛВС может мониторить потенциальные угрозы безопасности БЛВС из графического пользовательского интерфейса (GUI) сервера WIPS.

**РИСУНОК 16.10** Мониторинг WIPS



Системы WIPSs являются лучшими в мониторинге атак 2ого уровня, таких как подмена MAC [MAC spoofing], атаки диассоциацией, и атаки деаутентификацией. У большинства систем WIPS есть сигналы тревоги для 100 потенциальных рисков безопасности. Важная часть развертывания WIPS - это настройка политик и оповещений. Ложно-положительные срабатывания часто являются проблемой в системах обнаружения вторжений, но они могут быть меньшей проблемой, если определены надлежащие политики и пороги. Политики могут быть созданы, для определения различных сигналов тревоги и оповещений. Например, сигнал тревоги для широкого вещания [broadcasting] SSID может не считаться критичным и может быть даже отключен. Однако,

политика может быть настроена так, чтобы классифицировать атаки подмены деаутентификации как критичные, и сообщение электронной почты или текстовое SMS сообщение может быть автоматически отправлено сетевому администратору.

Хотя большая часть проверок, выполняемых WIPS, выполняется в целях безопасности, многие WIPS также имеют возможности мониторинга производительности. Например, сигналы тревоги о производительности могут быть в виде чрезмерной утилизации полосы или чрезмерных переассоциаций и роуминга телефонов VoWiFi.

Компоненты решения по мониторингу безопасности БЛВС обычно устанавливаются по одной из двух следующих основных архитектур WIPS:

**Устанавливаемая поверх [Overlay]** Большинство моделей защиты - это устанавливаемые поверх (или надстраиваемые) WIPS, которые устанавливаются поверх существующей беспроводной сети. Эта модель использует WIPS независимых производителей, и может быть развернута, чтобы мониторить любую существующую или планируемую БЛВС. Устанавливаемые поверх системы обычно имеют более расширенные функции, но они обычно и более дорогие. Устанавливаемые поверх решения состоят из сервера WIPS и сенсоров, которые не являются частью решения БЛВС, которое предоставляет доступ клиентам. Выделенные надстраиваемые системы не так широко распространены, как раньше; многие функции WIPS интегрированы в большинство продуктов корпоративных БЛВС.

**Интегрированная [Integrated]** У большинства производителей БЛВС есть полностью интегрированные функции WIPS. Центральный контроллер БЛВС или *центральная система управления сетью* [*network management server (NMS)*] работают как сервер WIPS. Решения WIPS также переносятся в облачные решения управления. Точки доступа могут быть настроены на постоянную работу [full-time] только в режиме сенсора или могут работать как временами [part-time] работающий сенсор, пока не передают как точки доступа. ТД используют процедуры внеканального [off-channel] сканирования в целях динамического управления радиоспектром. ТД также являются фактически временами [part-time] работающими сенсорами для встроенного сервера WIPS при прослушивании других каналов. Рекомендуемая практика - также устанавливать ТД как постоянно [full time] работающие сенсоры. Интегрированное решение менее дорогое решение, но у него может не быть всех возможностей устанавливаемой поверх [overlay] WIPS. Как упоминалось ранее, другой вариант может быть - это использование третьего радиомодуля, который работает все время как сенсор WIPS только в режиме прослушивания.

Одна из двух архитектур WIPS, интегрированная WIPS, намного более широко распространена. Устанавливаемые поверх WIPS обычно имеют заградительную стоимость для большинства заказчиков БЛВС. Более надежные устанавливаемые поверх решения WIPS обычно устанавливаются на предприятиях обороны, финансовых и вертикальных рынках крупной розничной торговли, где бюджет для поверх устанавливаемых решений может быть приемлемым.

## Обнаружение неучтенной ТД и уменьшение ее влияния

Как уже упоминалось, неучтенная [rogue] точка доступа - это любое неавторизованное Wi-Fi устройство, которое не находится под управлением соответствующих сетевых администраторов. Наиболее вызывающий беспокойство тип неавторизованных неучтенных

Wi-Fi устройств - это те, что подключены к проводной сетевой инфраструктуре.

Производители БЛВС используют разнообразные проводные и беспроводные методы обнаружения, чтобы определить подключена ли неучтенная точка доступа к проводной инфраструктуре. Некоторые методы обнаружения и классификации неучтенных подключений опубликованы, в то время как многие другие остаются проприетарными и торговыми секретами. Любое устройство 802.11, которое еще не авторизовано, автоматически будет классифицировано как неавторизованное (т.е. неразрешенное) устройство. Однако, классификация неучтенных [rogue] немного более сложная.

WIPS характеризует точки доступа и клиентские радиомодули по четырем или более классификациям. Хотя разные производители WIPS используют разную терминологию, некоторые примеры классификаций включают следующее:

**Авторизованное Устройство [Authorized Device]** Эта классификация относится к любой клиентской станции или точке доступа, которая является авторизованным (разрешенным) членом беспроводной сети компании. Сетевой администратор может вручную подписать каждый радиомодуль как авторизованное устройство после обнаружения системой WIPS или может импортировать список всех MAC адресов радиомодулей БЛВС компании в систему. Устройства также могут быть авторизованы скопом из файла с разделителями-запятыми. Интегрированные решения автоматически классифицируют любые ТД как авторизованные устройства. Интегрированное решение будет также автоматически классифицировать клиентские станции как авторизованные, если клиентские станции аутентифицированы надлежащим образом.

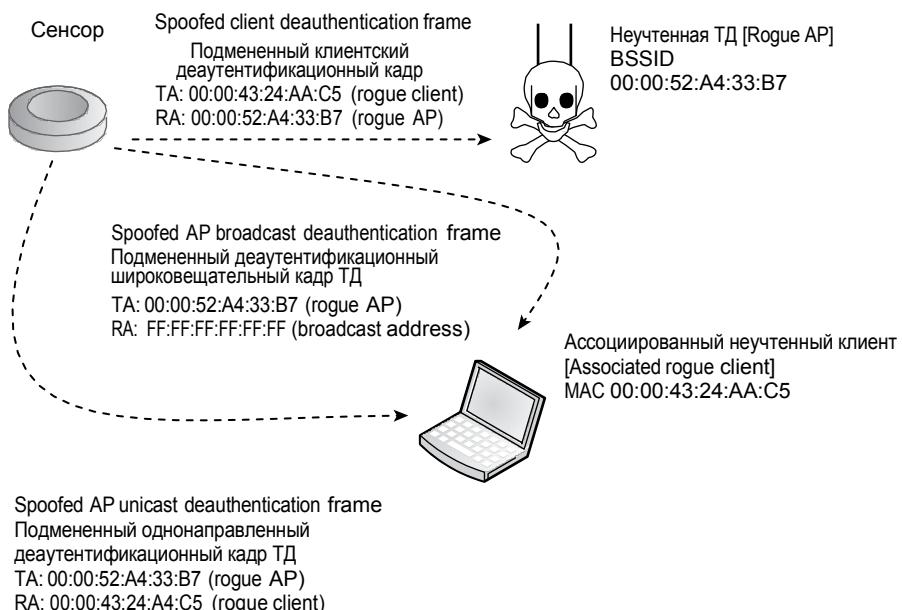
**Неавторизованное или Неизвестное Устройство [Unauthorized or Unknown Device]** Классификация неавторизованное устройство присваивается автоматически любому новому радиомодулю 802.11, который был обнаружен, но не классифицирован как неучтенный [rogue]. Неизвестные устройства считаются неавторизованными, и обычно исследуются дальше, чтобы определить являются ли они соседскими устройствами или потенциальной будущей угрозой. Неавторизованные устройства позже могут быть вручную классифицированы как известной соседней устройство.

**Соседнее Устройство [Neighbor Device]** Эта классификация относится к любой клиентской станции или точке доступа, которые обнаружены системой WIPS и чья личность известна. Этот тип устройств изначально обнаруживается как неавторизованное или неизвестное устройство. Маркировку соседнее устройство затем обычно присваивается вручную администратором. Устройства, классифицированные вручную как известные, наиболее часто являются точками доступа 802.11 или клиентскими радио устройствами соседнего предприятия, которые не считаются угрозой.

**Неучченное Устройство [Rogue Device]** Классификация неучтенный [rogue] относится к любой клиентской станции или точке доступа, которая считается интерферирующими устройством и потенциальной угрозой. Большинство решений WIPS определяет неучтенные точки доступа как устройства, фактически, включенные в проводную опорную сеть, но не известные или не управляемые организацией. Большинство производителей WIPS используют разнообразные методы, чтобы определить включена ли действительно неучтенная точка доступа в проводную инфраструктуру.

Большинство производителей WIPS используют различную терминологию при классификации устройств. Например, некоторые системы предотвращения беспроводных вторжений классифицируют все неавторизованные устройства как неучтенные [rogue] устройства, в то время как другие решения WIPS присваивают классификацию неучтенный [rogue] только ТД или устройствам БЛВС, для которых было обнаружено, что они включены в проводную сеть. После того, как клиентская станция или ТД классифицированы как неучтенные устройства, система WIPS может эффективно сдержать атаку. У производителей WIPS есть несколько способов осуществления этого. Один из наиболее широко распространенных методов – это использовать подмененные кадры деаутентификации [spoofed deauthentication frames]. Как показано на Рисунке 16.11, система WIPS заставляет сенсоры перейти в активный режим и начать передавать кадры деаутентификации, которые подставляют MAC адрес неучтенных ТД и неучтенных клиентов. WIPS использует известную атаку отказа-в-обслуживании 2ого уровня в качестве контрмеры. Эффект в том, что связь между неучтенней[rogue] ТД и клиентами становится бесполезной. Эта контрмера может быть использована для выключения неучтенных[rogue] ТД, индивидуальных клиентских станций, и неучтенных сетей «на лету» [ad hoc networks].

**РИСУНОК 16.11** Сдерживание неучтенных беспроводных подключений



Многие системы WIPSs также используют процесс завершения или терминации с проводной стороны, чтобы эффективно бороться с неучтенными устройствами. Метод терминации с проводной стороны борьбы с неучтенными включениями использует Простой Протокол Сетевого Управления [Simple Network Management Protocol (SNMP)] для погашения порта [*port suppression*]. Многие системы WIPS могут определить, что неучтенная ТД подключена к проводной инфраструктуре, и могут использовать SNMP для выключения порта управляемого коммутатора, к которому подключена неучтенная ТД. Если порт коммутатора не был закрыт, то атакующий мог получить доступ к сетевым ресурсам, которые находятся за неучтенной ТД.

У производителей систем WIPS есть и другие, часто неопубликованные, собственные методы выключения неучтенных ТД и клиентских станций. На текущий момент, главная цель WIPS - это сдерживание и отключение неучтенных устройств. В будущем, другие беспроводные атаки также могут быть отражены.



## Пример из Реальной Жизни

### Защитит ли WIPS от всех известных неучтенных устройств?

Простой ответ - нет. Хотя системы предотвращения беспроводного вторжения являются выдающимися продуктами, которые могут отразить многие атаки неучтенных подключений, некоторые неучтенные устройства останутся необнаруженными.

Радиомодули внутри сенсоров WIPS обычно мониторят полосу ISM 2,4 ГГц и частоты 5 ГГц U-NII. Каналы в диапазоне 4,9 ГГц, который зарезервирован для общественной безопасности в Соединенных Штатах и является действительной полосой каналов в Японии, часто также мониторятся на предмет потенциальных неучтенных устройств. Однако, существует устаревшее беспроводное сетевое оборудование, которое передает в полосе ISM 900 МГц также как и на других частотах. Эти устройства не будут обнаружены. Единственный инструмент, который на 100 процентов обнаружит точку доступа в 900МГц - это анализатор спектра, который работает на 900 МГц. Неучтенные ТД [Rogue APs], которые не передают ни в 2,4 ГГц, ни в 5 ГГц полосах частот не будут обнаружены стандартным решением WIPS для 802.11.

Не у всех WIPS есть функционал анализа спектра, хотя распределенный анализ спектра становится более распространенным. Даже если у WIPS есть функционал анализа спектра, он может проводить анализ спектра только в пределах поддерживаемых частот — это обычно те же самые частоты, которые он мониторит как WIPS сенсор. WIPS должен также мониторить все доступные каналы 2,4 и 5 ГГц, а не только те, которые разрешены в вашей стране нахождения.

## Анализаторы Спектра

Анализатор спектра [*spectrum analyzer*] это инструмент из области частот, который может обнаружить любой радиосигнал в сканируемом частотном диапазоне. Анализатор спектра, который мониторит полосу ISM 2,4 ГГц способен обнаружить и устройства преднамеренной постановки помех и непреднамеренной постановки помех. Некоторые анализаторы спектра могут посмотреть на радиосигнатуру интерферирующего сигнала и классифицировать устройство. Например, анализатор спектра может идентифицировать сигнал как излучение микроволновой печи, передатчик Bluetooth, или радиомодуль 802.11

FHSS. Доступны две формы систем анализа спектра: мобильная и распределенная. Большинство анализаторов спектра являются отдельными мобильными решениями. Многие производители корпоративных БЛВС предоставляют распределенный анализ спектра, используя возможности радиопрослушивания точек доступа, которые работают как сенсоры. *Распределенная система анализа спектра [distributed spectrum analysis system (DSAS)]* - фактически является системой обнаружения беспроводного вторжения на 1ом уровне и может классифицировать радиоинтерференцию. У системы DSAS есть возможность категоризировать типы интерференции на основе частотных сигнатур. Это может быть полезным в помощи классификации и локализации интерфеирирующих устройств. Большинство решений DSAS используют точки доступа для распределенного анализа спектра. Некоторые ТД производителей используют встроенные чипсеты анализатора спектра, которые работают независимо от радиомодуля 802.11. Другие производители используют радиомодуль 802.11 в точке доступа, чтобы выполнить анализ спектра низкого класса (грубый анализ).

## Политики Беспроводной Безопасности

Задача беспроводной сети и мониторинг угроз являются абсолютно необходимыми, но и то и другое бесполезно, если нет соответствующих политик безопасности. Что хорошего в решении 802.1X/EAP, если пользователи делятся своими паролями? Зачем покупать систему обнаружения вторжений, если у вас нет политики по борьбе с неучтенными ТД?

Все больше и больше предприятий начинают исправлять свои политики использования сети, чтобы включить в них раздел политики по беспроводной сети. Если вы еще этого не сделали, вы обязательно должны добавить раздел БЛВС в вашу корпоративную политику безопасности. Два хороших ресурса по знакомству с передовым опытом и политиками компьютерной безопасности это Институт SANS и Национальный Институт Стандартов и Технологий [National Institute of Standards and Technology (NIST)].



Шаблоны политик безопасности от Института SANS можно загрузить с [www.sans.org/resources/policies](http://www.sans.org/resources/policies). Можно также загрузить специально опубликованные документы NIST 800-153 и 800-97 относительно беспроводной безопасности с <https://csrc.nist.gov/publications>.

## Общие Политики Безопасности

При установке беспроводной политики безопасности вы сначала должны определить общую политику [*general policy*]. Общая политика беспроводной безопасности определяет зачем нужна политика беспроводной безопасности для организации. Даже если у компании нет планов по развертыванию беспроводной сети, должна быть минимум политика о том как поступать с неучтенными[*rogue*] беспроводными устройствами. Общая политика беспроводной безопасности определяет следующие пункты:

### Полномочия [Statement of Authority]

Полномочия определяют кто применяет беспроводную политику и исполнительное руководство, которое поддерживает политику.

**Целевая Аудитория [Applicable Audience]** Целевая аудитория - это аудитория, к которой применяется политика, например: сотрудники, посетители, и подрядчики.

**Процедуры Отчета о Нарушениях [Violation Reporting Procedures]** Процедуры отчета о нарушениях определяют как политика беспроводной безопасности будет приведена в исполнение, включая действия, которые должны быть приняты, и кто отвечает за соблюдение.

**Оценка Рисков и Анализ Угроз [Risk Assessment and Threat Analysis]** Оценка рисков и анализ угроз определяет потенциальные риски и угрозы беспроводной безопасности и финансовый удар по компании, в случае осуществления успешной атаки.

**Аудит Безопасности [Security Auditing]** Процедуры внутреннего аудита, а также необходимость независимого внешнего аудита, также должны быть определены.

## Рабочие Политики Безопасности

Рабочая или Функциональная политика [*functional policy*] также нужна, чтобы определить технические аспекты беспроводной безопасности. Рабочая политика безопасности устанавливает как защитить беспроводную сеть в терминах того, какое решение и какие действия нужны. Рабочая политика беспроводной безопасности определяет следующие пункты:

**Основы Политики [Policy Essentials]** Базовые процедуры безопасности, такие как политика по паролям, обучение, и соответствующее использование беспроводной сети являются основами политики и должны быть определены.

**Базовое Применение [Baseline Practices]** Базовое применение определяет минимальное применение беспроводной безопасности, такое как проверочные списки конфигураций/настроек, процедуры апробирования и испытаний, и так далее.

**Проектирование и Внедрение [Design and Implementation]** Определяет применяемые решения аутентификации, шифрования, и сегментации.

**Мониторинг и Реагирование [Monitoring and Response]** Определяет все процедуры обнаружения беспроводного вторжения и соответствующую реакцию.

## Соответствие Законодательству

У большинства стран есть обязательные правила о том, как защищать и делать безопасной связь передачи данных во всех правительственные организациях. В Соединенных Штатах NIST поддерживает Федеральные Стандарты Обработки Информации [Federal Information Processing Standards (FIPS)]. Особый интерес для беспроводной безопасности представляет стандарт FIPS 140-3, который определяет требования безопасности к модулям шифрования. Правительство США требует использовать подтвержденные модули шифрования для всей несекретной связи. Другие страны также признают стандарт FIPS 140-3 или имеют свои аналогичные правила.

В Соединенных Штатах существуют другие законодательные акты по защите информации и связи в определенных отраслях, включая следующие:

**HIPAA** Акт о Переносимости и Учета Медицинского Страхования [Health Insurance

Portability and Accountability Act (HIPAA)] устанавливает национальные стандарты для электронных транзакций медицинской информации [healthcare transactions] и национальные стандарты для провайдеров, полисов медицинского страхования, и сотрудников. Цель - защитить информацию о пациенте и обеспечить конфиденциальность.

**Sarbanes–Oxley** Акт Сарбейнса-Оксли [ Sarbanes–Oxley] от 2002 года определяет строгий контроль за процедурами корпоративного учета и аудита с целью корпоративной ответственности и расширенного раскрытия информации о финансовом состоянии.

**GLBA** Акт Грэмма - Лича - Блайли [ Gramm–Leach–Bliley Act (GLBA)] заставляет банки и финансовые институты уведомлять заказчиков о политике и практиках раскрытия информации о заказчике. Цель - защитить персональную информацию, такую как номера кредитных карт, номера Социального Стархования [Social Security], имена, адреса и так далее.



Все публикации FIPS можно найти онлайн на [csrc.nist.gov/publications/PubsFIPS.html](http://csrc.nist.gov/publications/PubsFIPS.html). Узнайте больше о HIPAA на [www.hhs.gov/hipaa/index.html](http://www.hhs.gov/hipaa/index.html). Вы можете найти общую информацию об акте Сарбейнса-Оксли на [www.sarbanes-oxley-101.com](http://www.sarbanes-oxley-101.com) и о GLBA на [www.ftc.gov](http://www.ftc.gov).

В 2015 году Европейский Союз принял законы, разработанные для защиты прав конфиденциальности граждан ЕС в отношении сбора и обработки их персональных данных. Действие Общего Регламента по Защите Данных [*General Data Protection Regulation (GDPR)*] началось 25 Мая 2018 года.

GDPR - это комплексный закон из 99 статей. Его принципиальная цель - гарантировать, чтобы организации с доступом к персональным данным граждан ЕС, обеспечивали защиту от вторжения в частную жизнь и утечек данных. GDPR усиливает безопасность и защиту персональных данных, давая гражданам ЕС более высокую степень контроля над своими персональными данными, и тем как они могут быть использованы в цифровой экономике. Независимо от местоположения, организации, которые собирают, хранят и обрабатывают персональные данные резидентов ЕС должны следовать GDPR. Больше информации о GDPR можно найти на <https://gdpr.eu>.

В 27 июля 2006 году в Российской Федерации был принят Федеральный закон РФ № 152-ФЗ «О персональных данных» по обеспечению защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

### Соответствие PCI [Индустрии Платежных Карт]

Чем больше нас полагается на кредитные карты как на основное платежное средство, тем больше мы рискуем потерять номера своих карт из-за атакующих и похитителей личных данных через незащищенную обработку и/или хранение нашей информации о держателе карты. Индустрия Платежных Карт [Payment Card Industry (PCI)] осознает, что для поддержания дальнейшего роста бизнеса, должны быть приняты меры по защите данных заказчиков и номеров карт. Совет по Стандартам Безопасности Индустрии Платежных Карт [PCI Security Standards Council (SSC)] внедрил правила для организаций обрабатывающих и хранящих информацию о держателях карт. Обычно это называется как *Стандарт Безопасности Данных PCI [PCI Data Security Standard]*. Текущая версия документа стандарта PCI-DSS вер. 4.0; однако, стандарт обновляется каждые три года. Внутри этого стандарта есть компоненты регулирующие использование беспроводных устройств. Больше информации о стандарте PCI можно найти на [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).

## Рекомендации по Беспроводной Политике 802.11

Хотя должен быть создан подробный и точный документ, мы настойчиво рекомендуем следующие шесть политик беспроводной безопасности

**Политика по устройствам сотрудников [BYOD Policy]** Сотрудники любят приносить свои персональные Wi-Fi устройства, такие как планшеты и смартфоны, на рабочее место. Сотрудники обычно ожидают, что они смогут использовать свои персональные Wi-Fi устройства в защищенной корпоративной БЛВС. Каждому работодателю нужно определить политику по использованию собственных устройств [*bring your own device (BYOD)*], которая четко описывает как персональные устройства могут быть приняты в безопасную корпоративную БЛВС. Политика BYOD должна также декларировать как персональные устройства могут использоваться, пока они подключены к БЛВС компании, и какие корпоративные сетевые ресурсы им доступны. BYOD обсуждается более подробно в Главе 18 "Использование собственных устройств (BYOD) и Гостевой Доступ."

**Политика Гостевого Доступа [Guest Access Policy]** Пользователи Гостевого Wi-Fi должны быть ограничены от доступа к большинству сетевых ресурсов компании. Гостевые пользователи должны быть ограничены от доступа к сетевым ресурсам компании с помощью сильного межсетевого экрана и применением сетевой сегментации. Также могут быть применены ограничения по качеству сервиса [QoS] и полосе. Гостевой БЛВС обсуждается более детально в Главе 18.

**Политика относительно БЛВС с общественным доступом [Public-Access WLAN Policy]** Конечные пользователи берут свои ноутбуки и ручные устройства и уходят с территории компании. Большинство пользователей вероятно используют беспроводные сети дома и на беспроводных хотспотах для доступа в Интернет. По проекту, на многих из этих удаленных беспроводных сетей абсолютно нет защиты, и крайне важно чтобы непременно применялась политика по использованию публично доступных БЛВС. Эта политика должна включать требование по использованию IPSec или SSL VPN решений для обеспечения аутентификации устройства, аутентификации пользователя, сильного шифрования всего беспроводного трафика данных. Хотспоты являются основными целями для злонамеренных атак подслушивания. На всех удаленных компьютерах

должны быть установлены персональные межсетевые экраны, чтобы предотвратить атаки равный-с-равным [peer-to-peer attacks]. Персональные межсетевые экраны не предотвратят атаки угона [hijacking attacks] или атаки равный-с-равным [peer-to-peer attacks], но они предотвратят доступ атакующих к вашей наиболее критичной информации. Существуют программные решения по принудительному применению политик для конечных точек БЛВС, которые заставляют конечных пользователей использовать безопасность VPN и межсетевого экрана при доступе к любой беспроводной сети, отличной от корпоративной БЛВС. Политика по использованию публичного доступа обязательна, потому что наиболее вероятное и уязвимое место для проведения атаки - это хотспот публичного доступа.

**Политика по неучтенным ТД [Rogue AP Policy]** Ни одному конечному пользователю не должно быть разрешено устанавливать свое собственное беспроводное устройство в корпоративную сеть. Это касается ТД, беспроводных маршрутизаторов, беспроводных аппаратных USB клиентов, и других сетевых карт БЛВС [WLAN NICs]. Любые пользователи, устанавливающие свое собственное беспроводное оборудование, могут открыть незащищенные порталы в главную инфраструктурную сеть. Эта политика должна строго соблюдаться. Конечным пользователям нельзя разрешать устанавливать сети "на лету" [ad hoc] или равный-с-равным [peer-to-peer]. Сети равный-с-равным [Peer-to-peer] чувствительны к атакам равный-с-равным [peer attacks] и могут работать как незащищенные порталы к инфраструктурной сети, если также используется Ethernet порт компьютера.

**Политика надлежащего использования Беспроводной ЛВС [Wireless LAN Proper Use Policy]** Тщательная политика должна описывать надлежащее использование и внедрение основной беспроводной корпоративной сети. Эта политика должна включать надлежащие процедуры установки, надлежащее внедрение защиты, и использование разрешенных приложений на беспроводной БЛВС.

**Политика по обнаружению вторжений [WIPS Policy]** Должны быть написаны политики, определяющие, как правильно реагировать на сигналы тревоги, создаваемые системой предотвращения беспроводного вторжения. Примером может быть описание того, как поступать с обнаружением неучтенной ТД, и все необходимые действия, которые нужно предпринять.

Эти шесть политик просты, но являются хорошей стартовой точкой в написании документа политики беспроводной безопасности.

## ИТОГО

В этой главе мы обсудили все потенциальные беспроводные атаки и угрозы. Неучтенная [rogue] точка доступа всегда была большим вопросом в терминах беспроводных угроз, за которой сразу следовала социальная инженерия. Мы обсудили много других серьезных угроз—таких как атаки равный-с-равным [peer-to-peer] и подслушивание [eavesdropping]—которые могут иметь серьезные последствия. Мы также обсудили атаки отказа-в-обслуживании [denial-of-service (DoS)], которые не могут быть отражены, а только могут быть отслеживаемы. Мы охватили различные решения, которые доступны для мониторинга вторжений. Большинство решений по обнаружению вторжений используют распределенную клиент-серверную модель, и некоторые предлагают функционал предотвращения неучтенного [rogue] подключения. Наконец, мы обсудили необходимость в качественных политиках беспроводной безопасности, которые действуют как основа для решений по беспроводной безопасности, которые вы внедряете.

# Темы Экзамена

**Понимать риск неучтенной точки доступа.** Уметь объяснить почему неучтенная [rogue] ТД предоставляет портал к сетевым ресурсам. Понимать, что сотрудники часто являются источником неучтенных ТД.

**Дать определение атак равный-с-равным [peer-to-peer].** Понимать, что атаки равный-с-равным [peer-to-peer] могут происходить через точку доступа или через сеть «на-лету» [ad hoc]. Объяснить, как защититься от этого типа атаки.

**Знать риски подслушивания.** Объяснить разницу между обычным и злонамеренным прослушиванием [eavesdropping]. Объяснить, почему шифрование необходимо для защиты.

**Дать определения атакам аутентификации и угона [hijacking].** Объяснить риски за этими типами атак. Понимать, что сильное решение 802.1X/EAP необходимо для борьбы с ними.

**Объяснить беспроводные атаки отказа-в-обслуживании [denial-of-service].** Знать разницу между DoS атаками уровня 1 и уровня 2. Объяснить почему с этими атаками не могут бороться, но можно только мониторить.

**Понимать типы решений по предотвращению беспроводного вторжения.** Объяснить назначение системы WIPS. Понимать, что большинство решений – это распределенные клиент-серверные модели. Знать различные компоненты решения мониторинга вторжения, а также различные модели. Понимать какие атаки можно мониторить, а какие можно предотвратить.

**Понимать необходимость политики беспроводной безопасности.** Объяснить разницу между общей и рабочей (функциональной) политиками.

## Контрольные Вопросы

1. Какая из этих атак считается атакой отказа-в-обслуживании [denial-of-service]? (Выберите все, что применимо.)
  - A. Человек по середине [Man-in-the-middle]
  - B. Постановка помех [Jamming]
  - C. Подмена деаутентификации [Deauthentication spoofing]
  - D. Подмена MAC [MAC spoofing]
  - E. Равный-с-Равным [Peer-to-peer]
2. Какая из этих атак будет считаться злонамеренным подслушиванием? (Выберите все, что применимо.)
  - A. NetStumbler
  - B. Равный-с-равным [Peer-to-peer]
  - C. Запись анализатора протокола [Protocol analyzer capture]
  - D. Реконструкция пакета [Packet reconstruction]
  - E. Поток PS-Poll [PS-Poll floods]
3. Какая из этих атак не будет обнаружена системой предотвращения беспроводного вторжения [wireless intrusion prevention system (WIPS)]?
  - A. Подмена деаутентификации [Deauthentication spoofing]
  - B. Подмена MAC [MAC spoofing]
  - C. Неучтенная точка доступа [Rogue access point]
  - D. Подслушивание анализатором протоколов [Eavesdropping with a protocol analyzer]
  - E. Поток ассоциаций [Association flood]
4. Какая из этих атак может быть уменьшена решением с взаимной аутентификацией? (Выберите все, что применимо.)
  - A. Злонамеренное подслушивание [Malicious eavesdropping]
  - B. Деаутентификация [Deauthentication]
  - C. Человек-по-середине [Man-in-the-middle]
  - D. Беспроводной угон [Wireless hijacking]
  - E. Поток аутентификаций [Authentication flood]
5. Какой тип безопасности может быть использован, чтобы остановить атакующих от просмотра MAC адресов, используемых вашими законными устройствами БЛВС 802.11?
  - A. Фильтрация по MAC [MAC filtering]
  - B. Шифрование CCMP/AES [CCMP/AES encryption]
  - C. Подмена MAC [MAC spoofing]
  - D. Борьба с неучтенным подключением [Rogue mitigation]

- E.** Обнаружение неучтенного подключения [Rogue detection]
  - F.** Ничего из вышеперечисленного [None of the above]
- 6.** Когда вы создаете документ беспроводной политики, какие две основные области политики следует рассмотреть?
  - A.** Общая политика [General policy]
  - B.** Рабочая политика [Functional policy]
  - C.** Политика о неучтенных ТД [Rogue AP policy]
  - D.** Политика аутентификации [Authentication policy]
  - E.** Физическая безопасность [Physical security]
- 7.** Что может случиться, когда вторгшийся скомпрометировал PSK или пароль, используемый во время аутентификации WPA/ WPA2-Personal? (Выберите все, что применимо.)
  - A.** Расшифровка [Decryption]
  - B.** Атака ASLEAP [ASLEAP attack]
  - C.** Подмена [Spoofing]
  - D.** Взлом шифрования [Encryption cracking]
  - E.** Доступ к сетевым ресурсам [Access to network resources]
- 8.** Какая из этих атак считается атакой DoS 2ого уровня? (Выберите все, что применимо.)
  - A.** Подмена деаутентификации [Deauthentication spoofing]
  - B.** Постановка помех [Jamming]
  - C.** Атаки на виртуальную несущую [Virtual carrier attacks]
  - D.** Поток запросов PS-Poll [PS-Poll floods]
  - E.** Поток аутентификаций [Authentication floods]
- 9.** Что из этого может вызвать непреднамеренную атаку постановки радиопомех против беспроводной сети 802.11? (Выберите все, что применимо.)
  - A.** Микроволновая печь [Microwave oven]
  - B.** Генератор сигналов [Signal generator]
  - C.** Беспроводной телефон в 2,4 ГГц [2.4 GHz cordless phones]
  - D.** Беспроводной телефон в 900 МГц [900 MHz cordless phones]
  - E.** Деаутентификационный передатчик [Deauthentication transmitter]
- 10.** Неучтенные[Rogue] устройства БЛВС в основном устанавливаются кем? (Выберите все, что применимо.)
  - A.** Атакующими [Attackers]
  - B.** Вардрайверами [Wardrivers]
  - C.** Подрядчиками [Contractors]
  - D.** Посетителями [Visitors]
  - E.** Сотрудниками [Employees]

11. Какие два решения помогают смягчить атаки равный-с-равным [peer-to-peer] от других клиентов, ассоциированных с той же самой точкой доступа 802.11?
- A. Персональный межсетевой экран [Personal firewall]
  - B. Шифрование WPA2 [WPA2 encryption]
  - C. Изолирование клиентов [Client isolation]
  - D. Фильтр по MAC [MAC filter]
12. Какой тип решения может быть использован чтобы принять контрмеры против неучтенной[rogue ] точки доступа?
- A. CCMP
  - B. PEAP
  - C. WIPS
  - D. TKIP
  - E. WINS
13. Система WIPS использует какие четыре маркировки для классификации устройств 802.11? (Выберите все, что применимо.)
- A. Авторизованная [Authorized]
  - B. Сосед [Neighbor]
  - C. Включена [Enabled]
  - D. Выключена [Disabled]
  - E. Неучтенная [Rogue]
  - F. Неавторизованная/неизвестная [Unauthorized/unknown]
14. Скотт - администратор в Вильямс Ламбер Кампани [Williams Lumber Company], и его система WIPS обнаружила неучтенную [rogue] точку доступа. Какие действия должны быть предприняты после того как WIPS обнаружила неучтенную [rogue] ТД? (Выберите два лучших ответа.)
- A. Включить функцию сдерживания неучтенного подключения на 2ом уровне, которую предоставляет система WIPS.
  - B. Отключить неучтенную [rogue] ТД из электрической розетки при нахождении.
  - C. Позвонить в полицию.
  - D. Позвонить его маме.
  - E. Отключить неучтенную [rogue] ТД от порта данных при нахождении.
15. Какой из этих атак подвержены беспроводные пользователи в общедоступном хотспоте? (Выберите все, что применимо.)
- A. Wi-Fi фишинг [Wi-Fi phishing]
  - B. Атака счастливая ТД [Happy AP attack]
  - C. Атака равный-с-равным [Peer-to-peer attack]
  - D. Злонамеренное подслушивание [Malicious eavesdropping ]
  - E. Атака небесных обезьян 802.11 [802.11 sky monkey attack]
  - F. Атака человек-по-середине [Man-in-the-middle attack]
  - G. Беспроводной угон [Wireless hijacking]

- 16.** Какие два компонента должны быть обязательными в каждой политике беспроводной безопасности при использовании публичного доступа? (Выберите два лучших ответа.)
- A.** Зашифрованная VPN [Encrypted VPN]
  - B.** 802.1X/EAP
  - C.** Персональный межсетевой экран [Personal firewall]
  - D.** Портал авторизации [Captive portal]
  - E.** Беспроводной электрошокер [Wireless stun gun]
- 17.** Фильтрация по MAC обычно считается применением слабой защиты из-за какого типа атаки?
- A.** Спам [Spamming]
  - B.** Подмена [Spoofing]
  - C.** Фишинг [Phishing]
  - D.** Взлом [Cracking]
  - E.** Подслушивание [Eavesdropping]
- 18.** Какая архитектура WIPS наиболее часто устанавливается?
- A.** Интегрированная [Integrated]
  - B.** Устанавливаемая поверх [Overlay]
  - C.** Доступ [Access]
  - D.** Ядро [Core]
- 19.** Какая из этих технологий шифрования была взломана? (Выберите все, что применимо.)
- A.** 64-bit WEP
  - B.** 3DES
  - C.** CCMP/AES
  - D.** 128-bit WEP
- 20.** Какое другое имя атаки по беспроводному угону [wireless hijacking attack]?
- A.** Wi-Fi фишинг [Wi-Fi phishing]
  - B.** Человек-по-середине [Man-in-the-middle]
  - C.** Фальшивая ТД [Fake AP]
  - D.** Злой двойник [Evil twin]
  - E.** AirSpy



# Глава **17**

A black and white photograph of a lighthouse situated on a rocky coastline. The lighthouse is white with a dark lantern room and is surrounded by several buildings, possibly keeper's houses. The foreground consists of large, light-colored rocks. The ocean waves are visible in the background under a cloudy sky.

# Архитектура Сетевой Безопасности 802.11

---

**В ЭТОЙ ГЛАВЕ ВЫ УЗНАЕТЕ О СЛЕДУЮЩЕМ:**

✓ **Основы безопасности 802.11**

- Конфиденциальность и целостность данных
- Аутентификация, авторизация и учет (AAA)
- Сегментация
- Мониторинг и политика

✓ **Устаревшая безопасность 802.11**

- Устаревшая аутентификация
- Статическое шифрование WEP
- MAC фильтры
- Сокрытие SSID

✓ **Надежная безопасность**

- Надежная защищенная сеть (RSN)
- Аутентификация и авторизация
- Аутентификация PSK
- Проприетарная аутентификация PSK
- Одновременная аутентификация равных (SAE)
- Структура 802.1X/EAP
- Типы EAP
- Динамическая генерация ключей шифрования
- 4x-Стороннее Рукопожатие
- Шифрование БЛВС
- Шифрование TKIP
- Шифрование CCMP
- Шифрование GCMP



- ✓ **Защита кадров управления**
- ✓ **WPA2**
- ✓ **WPA3**
  - WPA3-Personal
  - WPA3-Enterprise
- ✓ **Улучшенная Открытость [Enhanced Open]**
- ✓ **Безопасность Wi-Fi 6 ГГц**
- ✓ **Сегментация трафика**
  - VLANs
  - RBAC
- ✓ **Беспроводная безопасность с VPN**
  - Простой VPN
  - VPNы Зого уровня
  - SSL VPNs
  - Установка VPN



В этой главе вы узнаете об одной из наиболее обсуждаемых тем, касающихся беспроводных сетей 802.11: безопасность. В этой главе мы обсуждаем устаревшие решения безопасности 802.11, а также более надежные решения, которые теперь определены стандартом 802.11-2020. Безопасность БЛВС имела плохую репутацию в свои ранние годы—и это действительно так. Старые механизмы безопасности, изначально определенные IEEE, не обеспечивали адекватной аутентификации и конфиденциальности данных, которые нужны в мобильной среде. Хотя нет такого как 100 процентная безопасность, надлежащим образом установленные и управляемые решения существуют, которые могут укрепить и защитить вашу беспроводную сеть.

Как вы узнали из Главы 16 "Беспроводные Атаки, Мониторинг Вторжений, и Политика", существуют многочисленные риски беспроводной безопасности. Многие из атак против сети 802.11 могут быть отражены надлежащим внедрением архитектуры безопасности, обсуждаемой в этой главе. Однако, многие атаки не могут быть отражены и их можно только мониторить и, надеюсь, отреагировать.

Хотя менее 10 процентов экзамена CWNA охватывает безопасность 802.11, программа CWNP предлагает еще одну сертификацию, Сертифицированный Профессионал Беспроводной Безопасности [Certified Wireless Security Professional (CWSP)], которая сосредоточена как раз на теме беспроводной безопасности. Сертификационный экзамен CWSP более глубокого понимания безопасности 802.11. Однако, эта глава даст вам основы беспроводной безопасности, которые помогут вам пройти раздел безопасности экзамена CWNA, а также даст вам фору в знаниях, которые вам нужны для внедрения надлежащей беспроводной безопасности.

## Основы безопасности 802.11

Когда вы защищаете беспроводную сеть 802.11, обычно требуются следующие пять основных компонентов:

- Конфиденциальность и целостность данных
- Аутентификация, авторизация и учет (AAA)
- Сегментация
- Мониторинг
- Политика

Так как данные в эфире передаются свободно и открыто, то нужна соответствующая защита, чтобы обеспечить конфиденциальность данных, то есть нужно сильное шифрование. Функция большинства беспроводных сетей - это предоставить портал в некоторую другую сетевую инфраструктуру, такую как опорная сеть [backbone] Ethernet 802.3. Беспроводной портал должен быть защищенным, и, следовательно, нужно решение по аутентификации, чтобы гарантировать, что только авторизованные устройства и пользователи могут пройти через портал, через беспроводную точку доступа (ТД). После того как пользователи были авторизованы для прохождения через беспроводной портал, пользователи и клиентские устройства требуют дальнейшего ограничения доступа на основе идентификации для доступа к сетевым ресурсам.

Беспроводные сети 802.11 могут быть еще больше защищены непрерывным мониторингом системы предотвращения беспроводного вторжения. Все эти компоненты безопасности также должны быть объединены вместе с соблюдением политики.

Никогда не относитесь легкомысленно к сетевой безопасности проводной или беспроводной сети. К сожалению, безопасность БЛВС все еще имеет плохую репутацию у некоторых людей из-за слабых устаревших механизмов безопасности 802.11, которые были изначально развернуты. Однако, в 2004 году была принята поправка 802.11i и она определяла сильное шифрование и более лучшие методы аутентификации. Поправка 802.11i является частью стандарта 802.11-2020 и полностью определяет надежную безопасную сеть [robust security network (RSN)], которая обсуждается позже в этой главе. При обсуждении безопасности 802.11, сертификация безопасности WPA2/WPA3 Wi-Fi Альянса должна считаться финальной авторитетной защитой. Если развернуты надлежащее шифрование и решения аутентификации, то беспроводная сеть может быть настолько защищена насколько, если даже не больше чем, проводной сегмент сети.

Когда надлежащим образом применены пять компонентов безопасности 802.11, обсуждаемые в этой главе, они образуют твердую основу для защиты вашей БЛВС.

## Конфиденциальность и целостность данных

Беспроводные сети 802.11 работают в полосах частот, не требующих лицензии, и все передачи данных идут в открытом эфире. Защищать конфиденциальность данных в проводной сети намного легче, потому что физический доступ к проводной среде более ограничен, в то время как доступ к беспроводным передачам доступен каждому в зоне действия. Следовательно, использование технологий криптографического шифрования является обязательным для обеспечения надлежащей конфиденциальности данных.

*Шифр [cipher]* - это алгоритм, используемый для шифрования. Термин "криптология" выведен из Греческого языка и в переводе означает "скрытое слово". Цель криптологии - взять часть информации, часто называемой *открытый текст [plaintext]*, и, используя процесс или алгоритм, также называемый как ключ или шифр, преобразовать открытый текст в зашифрованный текст, также называемый шифротекст *[ciphertext]*. Наука маскировки открытого текста и затем его раскрытия называется *криптографией [cryptography]*. В компьютерной и сетевой отраслях процесс преобразования открытого текста в шифротекст обычно называется шифрованием *[encryption]*, а процесс преобразования шифротекста обратно в открытый текст обычно называется расшифровкой или дешифровкой *[decryption]*.

Два наиболее распространенных шифра, используемых для защиты данных - это *алгоритм ARC4 [ARC4 algorithm]* и алгоритм Улучшенный Стандарт Шифрования *[Advanced Encryption Standard (AES)]*. Некоторые шифры шифруют данные в непрерывный поток, в то время как другие шифруют данные по группам, называемые *блоками [blocks]*.

### Шифр ARC4

Алгоритм ARC4 - это потоковый шифр, используемый для защиты беспроводных данных 802.11 в двух устаревших методах шифрования, которые называются WEP и TKIP, оба обсуждаются позже в этой главе. ARC4 это сокращение от Alleged RC4 [в переводе означает: Предположительно RC4]. RC4 был создан в 1987 году Роном Ривестом [Ron Rivest] из компании RSA Security. Называется или как "Шифр Ривеста 4" ["Rivest Cipher 4"] или как "Код Рона 4" ["Ron's Code 4"]. RC4 изначально был коммерческой тайной; однако, в 1994 году его описание утекло в Интернет. Сравнительные испытания подтвердили, что утекший код был настоящим. RSA никогда официально не выпускала алгоритм, и название "RC4" -это торговая марка—поэтому, ее название ARCFOUR или ARC4.

## Шифр Улучшенного Стандарта Шифрования [Advanced Encryption Standard]

Алгоритм AES изначально назывался алгоритм Рейндал [Rijndael algorithm], это блочный шифр, который предлагает намного более сильную защиту, чем потоковый шифр ARC4. AES используется для шифрования беспроводных данных 802.11 используя метод шифрования с названием *Протокол Режима Счетчика с Кодом Аутентификации из Шифрованных Блоков Цепочки Сообщений [Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)]*, который также будет обсуждаться позже в этой главе. Алгоритм AES шифрует данные в фиксированные блоки данных с выбором силы ключа шифрования в 128, 192 или 256 бит. Шифр AES является обязательным алгоритмом правительства США для защиты и чувствительной и секретной информации. Шифр AES также используется для шифрования во многих других сетевых технологиях, например, IPsec VPNs.

В Главе 9 “802.11 MAC,” вы узнали о трех основных типах беспроводных кадров 802.11. Внутри тела кадра управления находится информация 2ого уровня, необходимая для базовой работы BSS, и исторически, кадры управления 802.11 не были зашифрованы. Однако, необходимость защиты некоторых критических сетевых функций, таких как аутентификация и ассоциация, была введена с поправкой 802.11w, которая обеспечивает защиту определенных типов кадров управления. У контрольных кадров нет тела, и они также не зашифрованы. Информация, которую нужно защитить - это информация верхних уровней внутри тела кадров данных 802.11. Если включено шифрование данных, блок сервисных данных MAC [MAC service data unit (MSDU)] внутри тела любого кадра данных 802.11 защищен шифрованием на 2ом уровне. Большинство методов шифрования, обсуждаемые в этой главе, используют шифрование на 2ом уровне, которое защищает информацию уровней 3-7, находящуюся внутри тела кадра данных 802.11. В упражнении 17.1 вы будете использовать анализатор протоколов 802.11, чтобы посмотреть на полезную нагрузку MSDU кадра данных 802.11.

### УПРАЖНЕНИЕ 17.1

#### Использование Нешифрованных и Зашифрованных Кадров Данных

- Чтобы выполнить это упражнение, вам нужно сначала загрузить файл CWNA CHAPTER17.PCAP с веб страницы книги по адресу [www.wiley.com/go/cwnasg6e](http://www.wiley.com/go/cwnasg6e).
- После того как файл загружен, вам нужна программа по анализу пакетов, чтобы открыть файл. Если у вас еще не установлен анализатор пакетов на вашем компьютере, загрузите Wireshark с [www.wireshark.org](http://www.wireshark.org).
- С помощью анализатора пакетов откройте файл CWNA CHAPTER17.PCAP. Большинство анализаторов пакетов показывают список записанных файлов в верхней секции экрана, где каждый кадр последовательно пронумерован в первом столбце.
- Прокрутите вниз список кадров и кликните по кадру #8, который является незашифрованным простым кадром данных. Посмотрите на тело кадра и обратите внимание на информацию верхних уровней, такую как IP адреса и TCP порты.
- Щелкните кадр #255, который является примером зашифрованного простого кадра данных. Посмотрите на тело кадра и заметьте, что используется шифрование CCMP, а информация верхних уровней не видна.

WEP, TKIP, и CCMP используют проверку целостности данных, чтобы гарантировать, что данные не были злонамеренно подменены. WEP использует значение проверки целостности [integrity check value (ICV)], а TKIP использует проверку целостности сообщения [message integrity check (MIC)]. CCMP также использует проверку целостности сообщения [message integrity check (MIC)], которая намного сильнее, чем методы целостности данных, используемые в TKIP или WEP.

## Аутентификация, авторизация и учет

*Аутентификация, авторизация и учет [Authentication, authorization, and accounting (AAA)]* – это ключевая концепция компьютерной безопасности, которая определяет защиту сетевых ресурсов

### Аутентификация [Authentication]

Аутентификация – это подтверждение личности [identity] и учетных данных [credentials]. Пользователи или устройства должны идентифицировать себя и предоставить учетные данные [credentials], такие как имена пользователей [usernames] и пароли [passwords] или цифровые сертификаты [digital certificates]. Более защищенные аутентификационные системы используют многофакторную аутентификацию, которая требует, чтобы по крайней мере два набора разных типов учетных данных были представлены.

### Авторизация [Authorization]

Авторизация определяет, авторизовано ли (разрешено ли) устройство или пользователь иметь доступ к сетевым ресурсам. Это может включать определение того можете ли вы иметь доступ на основе типа устройства, которое вы используете (ноутбук, планшет, или смартфон), ограничениях по времени дня, или местоположении. Прежде чем может быть определена авторизация, должна произойти надлежащая аутентификация.

### Учет [Accounting]

Учет – это отслеживание использования сетевых ресурсов пользователями и устройствами. Это важный аспект сетевой безопасности, используемый для сохранения исторического следа того, кто какие использовал ресурсы, когда и где. Запись хранит идентификацию пользователя, к каким ресурсам был доступ, и в какое время. Хранение учета о пользовании ресурсами [accounting trail] является требованием регулирующих правил многих отраслей, таких как индустрия платежных карт [payment card industry (PCI)].

Вспомните, что обычное назначение беспроводной сети 802.11 - действовать как портал в проводную сеть 802.3. Следовательно, необходимо защитить этот портал сильными методами аутентификации так, чтобы только законные пользователи с соответствующими учетными данными были допущены к сетевым ресурсам.

## Сегментация

Хотя это крайне важно защитить беспроводную сеть предприятия с использованием и сильного шифрования и решения AAA, также важный аспект беспроводной безопасности – это сегментация [Segmentation]- избранный метод по разделению

пользовательского трафика внутри сети. До введения сильных методов аутентификации и шифрования, беспроводная сеть рассматривалась как недоверенный [untrusted] сетевой сегмент. Следовательно, до принятия поправки безопасности 802.11i, весь беспроводной сегмент сети всеми считался как недоверенный [untrusted] сегмент, а проводная сеть 802.3 считалась доверенным [trusted] сегментом.

Теперь, когда существуют более безопасные решения, надлежащим образом защищенная БЛВС бесшовно и безопасно интегрируется в проводную инфраструктуру. Но все еще важно разделять пользователей и устройства по соответствующим группам, точно также как это делается на любой традиционной сети. Авторизовавшись на сетевых ресурсах, пользователи и устройства могут быть далее ограничены к каким ресурсам у них может быть доступ и куда они могут ходить. Сегментация может быть достигнута разными средствами, включая межсетевые экраны, маршрутизаторы, VPNы, VLANы, и методы инкапсуляции или туннелирования, такие как Обобщенная Маршрутизирующая Инкапсуляция [Generic Routing Encapsulation (GRE)]. Наиболее распространенная стратегия беспроводной сегментации, используемая в корпоративных БЛВС 802.11, это сегментация с помощью виртуальных ЛВС [virtual LANs (VLANs)]. Сегментация также переплетается с контролем доступа на основе ролей [role-based access control (RBAC)], которая обсуждается позже в этой главе.

## Мониторинг и Политика

После того как вы спроектировали и установили вашу беспроводную сеть, важно ее мониторить. В дополнение к мониторингу БЛВС на предмет ожиданий по производительности, обычно необходимо непрерывно мониторить БЛВС на предмет возможных атак и вторжений. Аналогично тому, как предприятия устанавливают видеокамеры снаружи здания, чтобы наблюдать пешеходный трафик входящий и выходящий через закрываемую дверь, так и администратору беспроводной сети нужно мониторить трафик защищенной беспроводной сети. Чтобы отследить потенциальную злонамеренную беспроводную активность на вашей сети, вы должны установить систему предотвращения беспроводного вторжения (WIPS). Мониторинг безопасности БЛВС может быть как встроенным решением, так и решением, устанавливаемым поверх. Решения по управлению сетью, которые включают мониторинг безопасности БЛВС, могут быть облачными или работать на частных серверах в data-центрах. Как обсуждалось в Главе 16, система WIPS также может отражать атаки от неучтенных [rogue] точек доступа и неучтенных клиентов путем проведения атаки против неучтенных устройств, фактически лишая их возможности взаимодействовать с вашей сетью.

## Устаревшая Безопасность 802.11

Исходный стандарт 802.11 мало определял в терминах безопасности. Методы аутентификации, впервые описанные в общих чертах в 1997 году, в основном представляли открытую дверь в сетевую инфраструктуру. Метод шифрования, определенный в исходном стандарте 802.11, долго был взламываемым и считался неподходящим для конфиденциальности данных. В следующих разделах вы узнаете о старых методах аутентификации и шифрования, которые были единственными стандартами для беспроводной безопасности 802.11 с 1997 года по 2004 год. Не смотря на то, что этим устаревшим механизмам безопасности уже более 15 лет, вы можете обнаружить, что эти небезопасные методы все еще используются на рабочих местах. Итак мы вам расскажем о

Позже в этой главе вы узнаете о более надежной защите, которая была определена в поправке безопасности 802.11i, которая теперь является частью текущего стандарта 802.11-2020. И мы обсудим также текущие механизмы безопасности, определенные для сертификации WPA2/WPA3 Wi-Fi Альянсом. Мы настойчиво рекомендуем уровни безопасности WPA2 или WPA3.

## Устаревшая Аутентификация

Вы уже знаете об устаревшей аутентификации из Главы 9. Исходный стандарт 802.11 определял два метода аутентификации: *аутентификация Открытой Системы [Open System authentication]* и *аутентификация с Общим Ключом [Shared Key authentication]*. При обсуждении аутентификации мы часто думаем о подтверждении личности [identity] пользователя, когда он подключается или входит в сеть. Аутентификация 802.11 очень отличается от этого. Эти устаревшие методы аутентификации были скорее не аутентификацией личности пользователя, а скорее аутентификацией способности. Думайте об этих методах аутентификации как о подтверждении между двумя устройствами того, что они оба являются устройствами 802.11. Аутентификация Открытой Системы [Open System] обеспечивает аутентификацию без проведения какого-либо типа подтверждения (проверки) пользователя. Это фактически двухсторонний обмен между клиентским радиомодулем и точкой доступа:

1. Клиент шлет аутентификационный запрос [authentication request].
2. Затем точка доступа шлет аутентификационный ответ [authentication response].

Так как аутентификация Открытой Системы [Open System authentication] не требует использование каких либо учетных данных [credentials], каждый клиент становится аутентифицированным и, следовательно, авторизованным для сетевых ресурсов, после того как ассоциируется. Статическое шифрование WEP является опциональным в аутентификации Открытой Системы и может быть использовано для шифрования кадров данных, после того как пройдет аутентификация Открытой Системы и ассоциация.

Как вы узнали из Главы 9, аутентификация с Общим Ключем [Shared Key authentication] использовала Конфиденциальность Эквивалентную Проводной [Wired Equivalent Privacy (WEP)] для аутентификации клиентских станций и требовала, чтобы статический WEP ключ был настроен и на станции и на точке доступа. В дополнение к тому, что WEP был обязателен, аутентификация могла не работать, если статические WEP ключи не совпадали. Аутентификационный процесс был сходным с аутентификацией Открытой Системы, но включал в себя еще вызов [challenge] и ответ [response] между радиокартами. Аутентификация с Общим Ключом была четырех-сторонним аутентификационным кадровым рукопожатием:

1. Клиентская станция посыпала запрос на аутентификацию [authentication request] точке доступа.
2. Точка доступа посыпала вызов открытым текстом [cleartext challenge] клиентской станции в аутентификационном ответе [authentication response].
3. Клиентская станция шифровала открытый текст вызова [cleartext challenge] и отправляла его обратно точке доступа в теле другого кадра с запросом на аутентификацию [authentication request frame].
4. Точка доступа расшифровывала ответ станции и сравнивала его с текстом вызова [challenge text]:

- Если они совпадали, точка доступа отвечала путем отправки четвертого и финального кадра аутентификации станции, подтверждая успех.
- Если они не совпадали, точка доступа отвечала отрицательно. Если точка доступа не могла расшифровать вызов [challenge], она также отвечала отрицательно.

Если аутентификация с Общим Ключом была успешной, тот же статический WEP ключ, который использовался во время аутентификации с Общим Ключом, также использовался для шифрования кадров данных 802.11.

### Открытая Система [Open System] или Общий Ключ [Shared Key]

Хотя аутентификация с Общим Ключом [Shared Key authentication] может показаться более безопасным решением, чем аутентификация Открытой Системы [Open System authentication], в действительности Общий Ключ может быть большим риском безопасности. Во время процесса аутентификации Общим Ключом любой, кто перехватит фразу вызова с открытым тестом [cleartext challenge phrase], а затем перехватит зашифрованную фразу вызова [encrypted challenge phrase] в ответном кадре, потенциально сможет вычислить статический WEP ключ. Если статический WEP ключ был скомпрометирован, откроется целая куча неприятностей, потому что теперь все кадры данных могут быть расшифрованы и атакующий может получить прямой доступ к сети. Ни один устаревший метод аутентификации не считается достаточно сильным для корпоративной безопасности. Аутентификация с Общим Ключом убрана и больше не рекомендуется. Более защищенные методы аутентификации 802.1X/EAP обсуждаются позже в этой главе.

## Статическое Шифрование WEP

Конфиденциальность Эквивалентная Проводной [Wired Equivalent Privacy (WEP)] это метод шифрования на 2ом уровне, который использует потоковый шифр ARC4. Исходный стандарт 802.11 определял только 64-битный WEP в качестве поддерживаемого метода шифрования. Затем вскоре также был определен 128-битный WEP в качестве поддерживаемого процесса шифрования. Три основные цели шифрования WEP:

### Конфиденциальность [Confidentiality]

Основная цель конфиденциальности - обеспечение конфиденциальности данных путем шифрования данных перед передачей.

### Контроль Доступа [Access Control]

WEP также обеспечивает контроль доступа, который по существу является грубой формой авторизации. Клиентским станциям, у которых не было того же самого соответствующего статического WEP ключа как и на точке доступа, отказывалось в доступе к сетевым ресурсам.

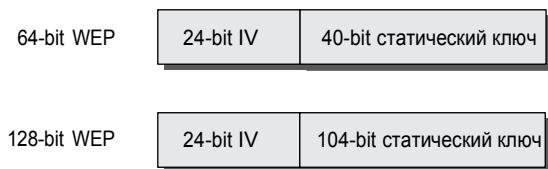
### Целостность Данных [Data Integrity]

Проверочная сумма целостности данных, называется как *значение проверки целостности* [integrity check value (ICV)], является вычисляемой по данным до шифрования и используется для защиты данных от изменения.

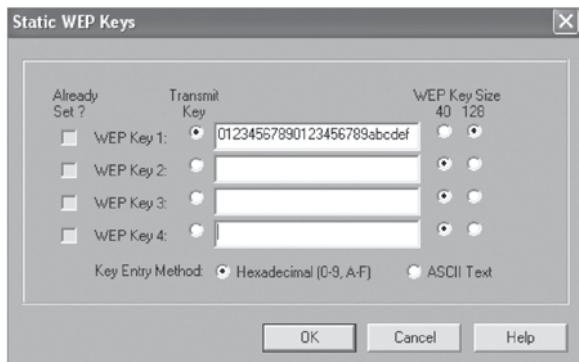
Хотя 128-bit WEP был подходящим, изначально правительство США разрешало экспорт только 64-битных технологий. После снятия правительством США экспортных ограничений на размер ключа, производители радиомодулей БЛВС начали производить

оборудование, которое поддерживает 128-битное WEP шифрование. Стандарт 802.11-2020 называет 64-битную версию как *WEP-40* а 128-битную версию как *WEP-104*. Как показывает Рисунок 17.1, 64-битная WEP использует секретный 40-битный статический ключ, который соединен с 24-битным числом, выбранным драйверами радиомодуля устройства. Это 24 битное число, называется *вектором инициализации* [*initialization vector (IV)*], посыпается открытым текстом, и новый вектор инициализации (IV) создается для каждого кадра. Хотя говорится, что вектор инициализации (IV) будет новым в каждом кадре, существует только 16 777 216 различных комбинаций вектора инициализации (IV); соответственно, вы вынуждены повторно использовать значения вектора инициализации (IV). Фактическая надежность ключа суммы вектора инициализации (IV) с 40-битным статическим ключом - это 64 битное шифрование. 128-битное WEP шифрование использует 104-битный секретный статический ключ, который также объединяется с 24-битным вектором инициализации (IV).

**РИСУНОК 17.1** Статический ключ шифрования WEP и вектор инициализации (IV)

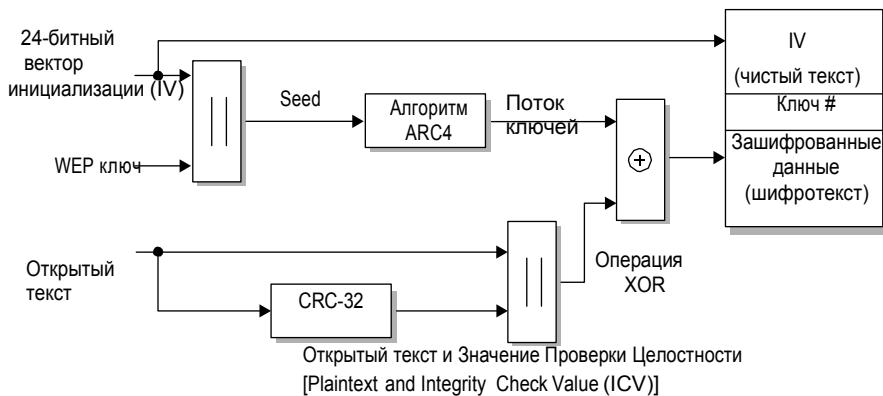


Статический WEP ключ обычно может вводиться или как шестнадцатеричные [hexadecimal (hex)] знаки (0–9 и A–F) или как знаки ASCII. Статический ключ должен совпадать и на точке доступа и на клиентском устройстве. 40-битный статический ключ состоит из 10 шестнадцатеричных [hex] знаков или 5 ASCII знаков, в то время как 104-битный статический ключ состоит из 26 шестнадцатеричных [hex] знаков или 13 ASCII знаков. Не все клиентские станции или точки доступа поддерживают и hex и ASCII. Многие клиенты и точки доступа поддерживают использование до четырех отдельных статических WEP ключей, из которых пользователь может выбрать один в качестве ключа передачи по умолчанию (Рисунок 17.2 показывает пример). Ключ передачи [*transmission key*] - это статический ключ, который используется для шифрования данных передающим радиомодулем. Клиент или точка доступа может использовать один ключ для шифрования исходящего трафика, а другой ключ для расшифровки принимаемого трафика. Однако, каждый из четырех ключей должен точно совпадать на обоих сторонах канала связи для надлежащей работы шифрования/дешифрования.

**РИСУНОК 17.2 Ключ передачи****Как работает WEP?**

1. WEP запускает циклическую резервную проверку [cyclic redundancy check (CRC)] открытого текста данных, который будет зашифрован, и прикрепляет значение проверки целостности [integrity check value (ICV)] в конце открытого текста данных.
2. Затем генерируется 24-битный открытый текст вектора инициализации (IV) и объединяется со статическим секретным ключом.
3. Затем WEP использует и статический ключ и вектор инициализации (IV) в качестве исходного материала для псевдо-случайного алгоритма, который генерирует случайные биты данных, называемые *потоком ключей* [keystream].  
Эти псевдослучайные биты являются одинаковыми по длине с открытым текстом данных, который должен быть зашифрован.
4. Затем псевдослучайные биты в потоке ключей [keystream] объединяются с битами открытого текста данных с помощью Булева процесса XOR [Boolean XOR process]. Конечный результат - шифротекст [ciphertext] WEP, который и есть зашифрованные данные.
5. Далее перед зашифрованными данными приставляется открытый текст вектора инициализации [cleartext IV]

Рисунок 17.3 иллюстрирует этот процесс.

**РИСУНОК 17.3** Процесс WEP шифрования

К сожалению, WEP имеет достаточно много слабостей, включая чувствительность к следующим четырем основным атакам:

#### **Атака столкновений векторов инициализации [IV Collisions Attack]**

Так как 24-битный вектор инициализации находится в открытом тексте [cleartext] и является разным в каждом кадре, то все 16 миллионов векторов инициализации (IV) очевидно будут повторяться в загруженной сети с WEP шифрованием. Из-за ограниченного размера пространства векторов инициализации [IV space], происходят коллизии или столкновения векторов инициализации, и атакующий может восстановить секретный ключ намного легче, когда в беспроводной сети происходят столкновения векторов инициализации [IV collisions].

#### **Атака на Слабый Ключ [Weak Key Attack]**

Из-за планирующего расписание ключей алгоритма ARC4, генерируются слабые ключи вектора инициализации (IV). Атакующий может восстановить секретный ключ намного проще путем восстановления известных слабых ключей вектора инициализации (IV).

#### **Атака Повторной Вставки [Reinjection Attack]**

Существуют хакерские инструменты, которые применяют атаку повторной вставки пакетов [packet reinjection attack], чтобы ускорить сбор слабых векторов инициализации (IVs) на сети с небольшим трафиком.

#### **Атака Манипулирования Битами [Bit-Flipping Attack]**

ICV проверки целостности данных считаются слабыми, т.е. недежными. Пакеты с WEP-шифрованием могут быть подделаны.

Инструменты по взлому WEP доступны много лет. Эти инструменты по взлому могут использовать комбинацию первых трех упомянутых атак и взломать WEP менее чем за 5 минут. После того как атакующий скомпрометирует статический WEP ключ, любой кадр данных может быть расшифрован с только что открытым ключом. Позже в этой главе мы обсуждаем TKIP, который является улучшением WEP. Шифрование CCMP использует алгоритм AES и является еще более надежным методом шифрования. Как определено исходным стандартом 802.11, WEP шифрование считается опциональным, т.е. необязательным. WEP был взломан и является неприемлемым методом шифрования для предприятий более 17 лет. Если устаревшие устройства, которые поддерживают только шифрование WEP все еще развернуты, то эти устройства нужно немедленно заменить.

### Динамическое WEP Шифрование

До 2004 года многие производители применяли решения, которые генерировали динамические ключи WEP шифрования в результате аутентификации 802.1X/EAP.

Динамические WEP никогда не были стандартизованы, но использовались производителями пока TKIP и CCMP не стали доступными на рынке.

Динамический WEP был решением по управлению коротко живущими ключами шифрования, которое часто внедрялось до выхода WPA-сертифицированных продуктов БЛВС. Создание и распространение динамических WEP ключей в результате процесса EAP аутентификации имело много преимуществ и было предпочтительнее, чем использование статических WEP ключей. Статические ключи больше не использовались и их не нужно было вводить вручную. Также, у каждого пользователя был отдельный независимый ключ. Если динамический пользовательский WEP ключ был скомпрометирован, то только трафик этого пользователя мог быть расшифрован. Однако, динамические WEP ключи все еще могли быть взломаны, и если скомпрометированы, то они действительно могли быть использованы для расшифровки кадров данных. У динамического WEP продолжали оставаться риски.

Пожалуйста, поймите, что динамический WEP ключ это не то же самое, что ключи шифрования TKIP или CCMP, которые также динамически генерируются. Позже в этой главе вы узнаете о ключах шифрования TKIP/ARC4 и CCMP/AES, которые динамически создаются процессом, называемом 4x-Стороннее Рукопожатие.

## MAC Фильтры

У каждой сетевой карты есть физический адрес, который называется MAC адрес [MAC address], произносится как мак адрес. Этот адрес - это 12-значное шестнадцатеричное число. У каждого радиомодуля 802.11 есть уникальный MAC адрес. Большинство производителей предоставляют возможности по MAC фильтрации на своих точках доступа. MAC фильтры могут быть настроены или на разрешение или на запрещение трафика от определенных клиентских MAC адресов при ассоциации и подключении к ТД.

Стандарт 802.11-2020 не определяет фильтрацию по MAC [MAC filtering], и любое применение фильтрации по MAC зависит от производителя. Большинство производителей используют MAC фильтры, чтобы запретить ассоциацию клиентов с ТД. Другие производители используют MAC фильтры межсетевых экранов, чтобы применить ограничения, которые разрешают пройти трафику только от определенных клиентских станций на основе их уникальных MAC адресов. Любые другие клиентские станции, чьи MAC адреса находятся не в разрешенном списке, не смогут пропустить трафик через виртуальный порт точки доступа в среду системы распространения. Стоит отметить, что MAC адреса могут быть подменены [spoofed], или подделаны, и любой хакер-любитель сможет легко пройти любой MAC фильтр путем подмены на разрешенный клиентский MAC адрес. Из-за подмены и из-за всей административной работы, вовлеченной в настройку MAC фильтров, фильтрация по MAC [MAC filtering] не считается надежным средством защиты для беспроводных сетей предприятий. MAC фильтры могут быть использованы как мера безопасности для защиты устаревших радиомодулей, которые не поддерживают более сильную безопасность. Например, старые ручные сканеры штрихкодов могут использовать радиомодули 802.11, которые поддерживают только статический WEP. Передовой опыт предписывает дополнительный уровень защиты путем отделения ручных устройств в отдельный VLAN с MAC фильтром на основе OUI адреса производителя (первые три октета MAC адреса, которые относятся к производителю).

## Сокрытие SSID

Помните в фильме «Звездный Путь» [Star Trek], когда Ромулане прятали свой звездолет, но Капитан Кирк каким-то образом всегда все-равно находил корабль? Хорошо, существует способ “спрятать” [“cloak”] ваш идентификатор состава сервиса (SSID). У точек доступа обычно есть настройка, называемая закрытая сеть [closed network], скрытый SSID [hidden SSID], или скрытый режим [stealth mode]. Включая эту функцию, вы можете спрятать [hide] или скрыть [cloak] название вашей беспроводной сети.

Когда вы внедряете закрытую сеть [closed network], поле SSID в кадре маяка пустое [null (empty)], и, следовательно, пассивное сканирование не покажет SSID клиентской станции, которая слушает маяки. SSID, который часто называется ESSID, это логический идентификатор БЛВС. Идея, стоящая за сокрытием SSID в том, что любая клиентская станция, которая не знает SSID БЛВС, не сможет обнаружить БЛВС и, следовательно, не ассоциируется, то есть не присоединиться.

Многие программные утилиты беспроводных клиентов передают зондирующий запрос [probe requests] с пустым [null] полем SSID при активном сканировании при поиске точек доступа. Кроме того, существует много популярных приложений обнаружения БЛВС, такие как inSSIDer, WiFi Explorer, и WiFi Analyzer, которые могут быть использованы отдельными людьми для обнаружения беспроводных сетей. Большинство из этих приложений обнаружения также посыпают пустые зондирующие запросы [null probe requests] при

активном сканировании точек доступа. Когда вы внедряете закрытую сеть [closed network], то точка доступа отвечает на пустые зондирующие запросы [null probe requests] зондирующими ответами [probe responses]; однако, так как в кадре маяка, поле SSID пустое, то, следовательно, SSID невидим для клиентских станций, которые используют активное сканирование. Реализации закрытой сети [closed network] различаются между производителями БЛВС; точки доступа некоторых производителей могут просто игнорировать пустые зондирующие запросы [null probe requests], когда настроена закрытая сеть [closed network].

Фактически, ваша беспроводная сеть временно невидима, или скрыта. Заметьте, что точка доступа в закрытой сети [closed network] будет отвечать любой настроенной клиентской станции, которая передает направленные зондирующие запросы [directed probe requests] с правильно настроенным SSID. Это гарантирует, что законные конечные пользователи смогут аутентифицироваться и ассоциироваться с ТД. Однако, любая клиентская станция, которая не настроена на корректный SSID, не сможет аутентифицироваться или ассоциироваться.

Хотя включение закрытой сети может скрыть ваш SSID от некоторых таких инструментов обнаружения БЛВС, любой с беспроводным анализатором протоколов на 2ом уровне может перехватить кадры, передаваемые любым законным конечным пользователем, и найти SSID, который передается открытым текстом. Другими словами, скрытый SSID может быть найден, обычно за секунды, соответствующими инструментами. Многие профессионалы по беспроводной связи будут утверждать, что скрытие SSID – это пустая траты времени, в то время как другие рассматривают закрытую сеть как еще один уровень защиты.

Хотя вы можете скрыть ваш SSID, чтобы скрыть идентификацию вашей беспроводной сети от хакеров-новичков (часто называемых *мамкиными хакерами* [*script kiddies*]) и не хакеров, следует четко осознавать, что скрытие SSID не является окончательным средством решения беспроводной безопасности. Стандарт 802.11 не определяет скрытие SSID [SSID cloaking], поэтому все реализации [закрытой сети] зависят от конкретного производителя. В результате, несовместимость потенциально может стать причиной проблем подключения. Некоторые беспроводные клиенты не подключаются к скрытому SSID, даже если вручную введут SSID в клиентском программном обеспечении.

Следовательно, обязательно узнайте характеристики ваших устройств, прежде чем внедрять закрытую сеть. Скрытие SSID может также стать административной проблемой и проблемой поддержки. Требование к конечным пользователям настраивать SSID в программном интерфейсе радиомодуля, часто приводит к большему количеству звонков в поддержку, из-за неправильно настроенного SSID. Мы настойчиво рекомендуем, чтобы вы никогда не скрывали ваш SSID, а наоборот вещали ваш SSID для всех и каждого, чтобы все видели.

## Надежная Безопасность

В 2004 году была принята поправка безопасности 802.11i и теперь является частью стандарта 802.11-2020. Стандарт 802.11-2020 определяет метод аутентификации уровня предприятий, а также метод аутентификации для домашнего использования. Текущий стандарт определяет использование аутентификации 802.1X/ EAP, а также использование предварительно известного общего ключа [preshared key (PSK)] или пароля [passphrase]. 802.1X/EAP это надежный метод аутентификации, наиболее часто применяемый на предприятиях. Менее сложная аутентификация PSK обычно используется в средах небольших и домашних офисов [small office, home office (SOHO)], но может быть установлена и на предприятиях. Стандарт 802.11-2020 также требует использовать сильные, динамически методы генерирования ключей шифрования. Шифрование CCMP/AES является методом шифрования по умолчанию, а TKIP/ARC4 является optionalным методом шифрования.

До ратификации поправки 802.11i Wi-Fi Альянс представил сертификацию *Защищенный Wi-Fi Доступ* [*Wi-Fi Protected Access (WPA)*] как срез еще не выпущенной поправки 802.11i, поддерживающий только динамическую генерацию ключей шифрования TKIP/ARC4. Аутентификация 802.1X/EAP предназначалась для предприятий, а аутентификация по паролю [passphrase] предлагалась для сред SOHO.

После ратификации 802.11i, Wi-Fi Альянс представил сертификацию WPA2. *WPA2* это более полная реализация поправки 802.11i и поддерживает динамическое создание ключей шифрования и CCMP/AES и TKIP/RC4. Аутентификация 802.1X/EAP является более сложной и предназначена для предприятий, когда аутентификация по паролю проще и предназначена для SOHO среды. Любые радиомодули 802.11, произведенные после 2005 года скорее всего являются WPA2 совместимыми. Если радиомодуль WPA совместимый, он вероятнее всего поддерживает только шифрование TKIP/ARC4. Если радиомодуль WPA2 совместимый, он поддерживает более сильное динамическое шифрование CCMP/AES. Таблица 17.1 предлагает ценное сравнение различных стандартов безопасности 802.11 и сертификаций безопасности Wi-Fi Альянса.

**ТАБЛИЦА 17.1 Сравнение стандартов и сертификаций безопасности**

| IEEE              | Сертификация Wi-Fi Альянса                  | Метод Аутентификации      | Метод Шифрования    | Шифр            | Генерация Ключей |
|-------------------|---------------------------------------------|---------------------------|---------------------|-----------------|------------------|
| 802.11 legacy     | None                                        | Open System or Shared Key | WEP                 | ARC4            | Static           |
| 802.11-2020 (RSN) | WPA-Personal                                | Preshared key             | TKIP                | ARC4            | Dynamic          |
|                   | WPA-Enterprise                              | 802.1X/EAP                | TKIP                | ARC4            | Dynamic          |
|                   | WPA2-Personal                               | Preshared key             | CCMP<br>(mandatory) | AES (mandatory) | Dynamic          |
| WPA3-Personal*    | Simultaneous Authentication of Equals (SAE) | CCMP (mandatory)          | TKIP (optional)     | ARC4 (optional) | Dynamic          |
|                   |                                             |                           | TKIP (optional)     | ARC4 (optional) | Dynamic          |
|                   | WPA3-Enterprise*                            | 802.1X/EAP                | CCMP (mandatory)    | AES (mandatory) | Dynamic          |

\* Существует несколько режимов работы и для WPA3-Personal и для WPA3-Enterprise.

## Надежная Защищенная Сеть

Стандарт 802.11-2020 определяет, что называется, *надежные защищенные сети* [*robust security networks (RSNs)*] и *ассоциации надежных защищенных сетей* [*robust security network associations (RSNAs)*]. Две станции (STAs) должны аутентифицировать и ассоциировать друг друга, а также создать динамические ключи шифрования в процессе, известном как 4x-Стороннее Рукопожатие. Эта ассоциация между двумя станциями называется RSNA. Другими словами, любые два радиомодуля должны обменяться динамическими ключами шифрования, которые являются уникальными между этими двумя радиомодулями. Шифрование CCMP/AES является обязательным методом шифрования, а TKIP/ARC4 – опциональным методом шифрования.

Надежная защищенная сеть [*robust security network (RSN)*] позволяет создание только ассоциаций надежной защищенной сети [*robust security network associations (RSNAs)*]. RSN можно идентифицировать по полю, находящемуся в кадрах управления 802.11. Это поле называется *информационный элемент RSN* [*RSN information element (IE)*].

Информационный элемент является опциональным полем переменной длины, которое может быть найдено в кадрах управления 802.11. Поле информационного элемента RSN всегда находится в четырех разных кадрах управления 802.11: кадрах управления типа маяк [*beacon management frames*], кадрах зондирующего запроса [*probe response frames*], кадрах запроса на ассоциацию [*association request frames*], и кадрах запроса на переассоциацию [*reassociation request frames*].

Информационный элемент RSN также может находиться в кадрах ответах на переассоциацию [reassociation response frames], если включены функции 802.11r на ТД и на роуминговом клиенте. Это поле идентифицирует набор шифра [cipher suite] и возможности аутентификации каждой станции. Стандарт 802.11-2020 допускает создание ассоциаций предшествующих надежной защищенной сети [pre-robust security network associations (pre- RSNAs)], так же как и RSNAs. Другими словами устаревшие меры безопасности могут поддерживаться в том же самом базовом составе сервиса [basic service set (BSS)] вместе с механизмами, определенными для RSN безопасности. *Сети переходной безопасности [transition security network (TSN)]* поддерживают безопасность, определенную для RSN [RSN-defined security], а также устаревшую безопасность, такую как WEP, в одном и том же BSS, хотя многие производители не поддерживают TSN.

## Аутентификация и Авторизация

Как вы узнали ранее в этой главе, аутентификация – это подтверждение личности и учетных данных пользователя или устройства. Пользователи и устройства должны идентифицировать себя и представить учетные данные, такие как пароли или цифровые сертификаты. Авторизация зависит от того, разрешен ли пользователю или устройству доступ к сетевым ресурсам и сервисам. До того, как может быть предоставлена авторизации к сетевым ресурсам, должна состояться надлежащая аутентификация.

Следующие разделы детализируют более продвинутые аутентификационные и авторизационные средства защиты. Вы также узнаете, что возможности динамического шифрования возможны как побочный продукт этих сильных решений аутентификации.

## Аутентификация PSK

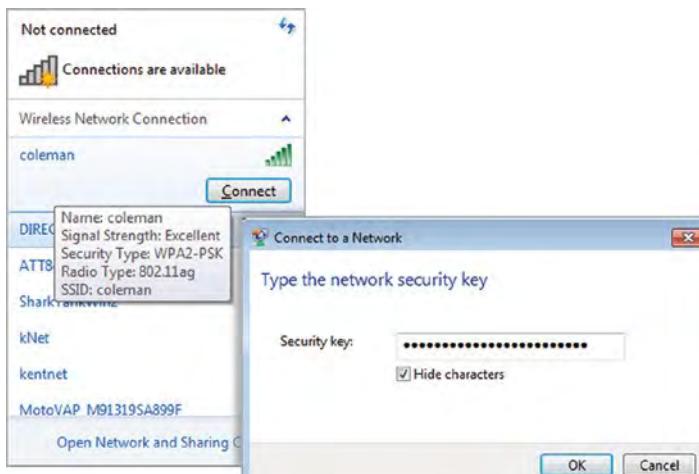
Стандарт 802.11-2020 определяет сервисы аутентификации и управления ключами [authentication and key management (AKM)]. Сервисы AKM требуют и процесс аутентификации, и генерацию и управление ключами шифрования. *Протокол аутентификации и управления ключами [authentication and key management protocol (AKMP)]* может быть или предварительно известным общим ключом [preshared (PSK)], или протоколом EAP, используемым во время аутентификации 802.1X/EAP. 802.1X/EAP требует наличие RADIUS сервера и продвинутого мастерства по его настройке и поддержке. У среднестатистического домашнего или малого бизнеса Wi-Fi пользователя нет знаний о 802.1X/EAP и нет RADIUS сервера в его гостиной. Аутентификация PSK подразумевается для использования в SOHO средах, потому что более сильные корпоративные решения аутентификации 802.1X/EAP не доступны. Более того, многие потребительского класса Wi-Fi устройства, такие как принтеры, не поддерживают 802.1X/EAP, а поддерживают только аутентификацию PSK. Следовательно, безопасность, используемая в SOHO средах - это *аутентификация PSK [PSK authentication]*.

WPA/WPA2-Personal использует аутентификацию PSK. С другой стороны, WPA/WPA2-Enterprise относится к аутентификации 802.1X/EAP.

Большинство беспроводных SOHO сетей защищены механизмами WPA/WPA2-Personal. До того, как IEEEratифицировал поправку 802.11i, Wi-Fi Альянс представил сертификацию Защищенный Доступ в Wi-Fi [Wi-Fi Protected Access (WPA)] как срез еще не выпущенной поправки 802.11, но она поддерживала только динамическое создание ключей шифрования TKIP/ARC4. Аутентификация 802.1X/EAP предлагалась для предприятий, в то время как метод аутентификация по паролю, названный WPA-Personal, был предлагаемым механизмом безопасности для домашних пользователей.

Предполагаемая цель WPA-Personal была в уходе от статических ключей шифрования к динамически генерируемым ключам, с использованием пароля [passphrase] в качестве исходного материала [seed]. Заранее известный общий ключ [preshared key (PSK)] используемый в надежной защищенной сети [robust security network] имеет 256 бит в длину, или 64 символа в шестнадцатеричной системе [hex]. PSK это статический ключ, который настроен на точке доступа и на всех клиентах. Один и тот же статический PSK используется всеми участниками базового состава сервиса [basic service set (BSS)]. Проблема в том, что среднестатистическому домашнему пользователю не удобно вводить 64 шестнадцатеричных символа PSK и на протребительского класса Wi-Fi маршрутизаторе и в клиентской утилите на ноутбуке. Даже если домашние пользователи ввели 64 символа PSK с обоих сторон, они вероятно не смогут запомнить этот PSK и будут его записывать. Большинству домашних пользователей, однако, очень удобно настраивать короткие ASCII пароли или парольные фразы [passphrases]. WPA/WPA2-Personal позволяет конечному пользователю ввести простую строку из ASCII символов, называемую парольной фразой [passphrase], любой длины от 8 до 63 символов. За кулисами, функция отображения пароль-в-PSK [passphrase-to-PSK mapping function] заботится обо всем остальном, преобразуя пароль [passphrase] в 256-битный PSK. Как показано на Рисунке 17.4, пользователи вводят статический пароль, от 8 до 63 символьную строку, в клиентскую программную утилиту на устройстве конечного пользователя и также на точке доступа. Пароль, используемый на всех устройствах должен совпадать.

**РИСУНОК 17.4** Клиент, настроенный со статическим паролем.



Как ранее упоминалось, формула *отображения пароль-PSK [passphrase-PSK mapping]* определена стандартом 802.11-2020, чтобы позволить конечным пользователям использовать простой ASCII пароль, который затем конвертируется в 256-битный PSK. Вот краткий обзор формулы преобразования пароля в PSK, с последующим объяснением процесса:

$$\text{PSK} = \text{PBKDF2}(\text{PassPhrase}, \text{ssid}, \text{ssidLength}, 4096, 256)$$

Простой пароль объединяется с SSID и хэшируется 4096 раз, чтобы произвести 256-битный (64 символьный) PSK. Таблица 17.2 иллюстрирует некоторые примеры того, как формула использует и пароль [passphrase] и SSID для генерации PSK.

**ТАБЛИЦА 17.2** Отображение пароль-PSK

| Пароль<br>(8–63 Символов) | SSID | 256-битный/64-Символьный PSK                                         |
|---------------------------|------|----------------------------------------------------------------------|
| Carolina                  | cwna | 7516b6d5169ca633есебaa43e0ca9d5c0afa08268ab9fde47c38a<br>627546b71c5 |
| certification             | cwna | 51da37d0c6ebba86123a13fb1ab0a1755a22fc9791e53fab7208a<br>5fce6038a2  |
| seahawks                  | cwna | 20829812270679e481067e149dbe90ab59b5179700c<br>6359ba534b240acf410c3 |

Весь смысл формулы преобразования пароль-PSK [passphrase-PSK mapping formula] в упрощении настройки для среднестатистического домашнего пользователя. Большинство людей могут запомнить 8ми символьный пароль, а не 256-битный PSK. Позже в этой главе вы узнаете, что существует симбиотическая связь между PSK, SAE, и 802.1X/EAP аутентификацией с генерацией динамических ключей шифрования в процессе 4x Стороннего Рукопожатия [4-Way Handshake]. 256-битный PSK также используется как парный мастер ключ [pairwise master key (PMK)]. PMK - это исходный материал [seeding material] для 4x Стороннего Рукопожатия, который используется для создания динамических ключей шифрования. Следовательно, PSK в режиме WPA/WPA2-Personal буквально тоже самое, что и PMK.

В Июне 2004 года рабочая группа IEEE 802.11 TGi формально ратифицировала 802.11i, которая добавила поддержку шифрования CCMP/AES. Wi-Fi Альянс модернизировал предыдущую спецификацию WPA до WPA2 и включил шифр CCMP/AES. Таким образом, единственное практическое различие между WPA и WPA2 заключается в шифре шифрования. WPA-Personal и WPA2-Personal используют метод аутентификации PSK; однако, WPA-Personal определяет шифрование TKIP/ARC4, в то время как WPA2-Personal определяет CCMP/AES.

Шифрование TKIP медленно уходило с годами, и не поддерживается для любой из 802.11n, 802.11ac, или 802.11ax скоростей передачи данных. Другими словами, WPA-Personal с TKIP не был вариантом выбора метода безопасности более 10 лет. К сожалению, вы можете найти старые клиентские устройства 802.11/a/b/g, которые поддерживают только WPA-Personal и TKIP и все еще развернуты на предприятиях.

Любые радиомодули 802.11, произведенные после 2006 года будут сертифицированы для WPA2-Personal и используют шифрование CCMP/AES. Если аутентификация PSK является выбранным методом безопасности, то всегда следует использовать шифрование WPA2-Personal с CCMP/AES.

Как вы узнали из Главы 16, аутентификация PSK подвержена оффлайновой усиленной атаке перебора по словарю. Следовательно, и IEEE и Wi-Fi Альянс рекомендуют очень сложный пароль в 20 символов или больше, когда применяется решение WPA2-Personal. Позже в этой главе мы обсудим WPA3-Personal, который меняет аутентификацию PSK на улучшенный процесс защиты [enhanced security process].

Официальное название Wi-Fi Альянса для аутентификации PSK - это WPA-Personal или WPA2-Personal. Однако, у производителей БЛВС много маркетинговых названий для аутентификации PSK, включая WPA/WPA2-Passphrase, WPA/WPA2-PSK, и WPA/WPA2-Preshared Key.

## Проприетарная Аутентификация PSK

Несмотря на то, что WPA2-Personal заменил WPA-Personal более 15 лет назад, держите в уме, что простой метод аутентификации PSK, определенный для WPA2-Personal, все еще слабый метод аутентификации, который уязвим для усиленных оффлайн атак перебора по словарю [brute-force offline dictionary attacks]. Еще хуже что, из-за того, что пароль является статическим, аутентификация PSK также чувствительна к атакам социальной инженерии.

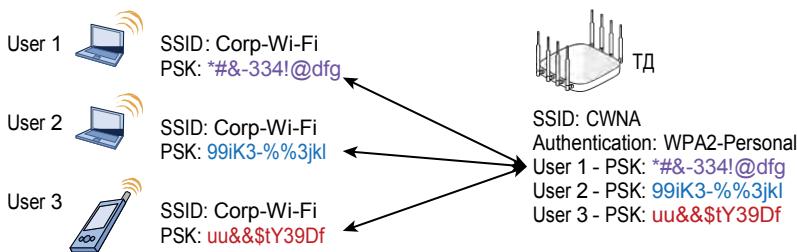
Хотя пароли и аутентификация PSK предназначены для использования в SOHO среде, в реальности WPA2-Personal часто используется на предприятиях. Например, хотя механизмы быстрого безопасного роуминга [fast secure roaming (FSR)] существуют уже некоторое время, некоторые старые VoWiFi телефоны и другие ручные устройства все еще не поддерживают 802.1X/EAP. Дополнительно, многие IoT устройства с Wi-Fi радиомодулями не поддерживают 802.1X/EAP. Как результат, самый сильный уровень безопасности, используемый этими устройствами - аутентификация PSK. Вопрос стоимости может также сподвигнуть небольшие предприятия использовать более простое решение WPA2-Personal, а не установку, настройку и поддержку RADIUS сервера для 802.1X/EAP.

В Главе 16, вы узнали, что аутентификация PSK уязвима к усиленным оффлайн атакам перебора по словарю. Однако большей проблемой с использованием аутентификации PSK на предприятиях является социальная инженерия. Так как пароль WPA2 статический, аутентификация PSK остро чувствительна к атакам социальной инженерии. PSK один и тот же на всех Wi-Fi устройствах. Если конечный пользователь, случайно, даст PSK хакерам, то безопасность БЛВС скомпрометирована. Если сотрудник уходит из компании, то чтобы поддержать безопасную среду, на всех устройствах нужно перенастроить 256-битный PSK. Поскольку пароль или PSK является общим для всех, то должна быть установлена строгая политика, гласящая, что только администратор по безопасности БЛВС отвечает за пароль или PSK. Что, конечно, создает другие административные проблемы, так как работа включает ручную настройку каждого устройства.

Несколько производителей корпоративных БЛВС предложили креативные решения по использованию WPA2-Personal, которые решают некоторые из самых больших проблем использования единого пароля для доступа в БЛВС. Каждое вычислительное устройство будет иметь свой собственный уникальный PSK для БЛВС. Следовательно, MAC адрес каждой STA будет ставится в соответствие с уникальным паролем WPA2-Personal. База данных соответствий уникальных PSK к именам пользователей или клиентским станциям должна храниться на всех точках доступа или на центральном сервере управления. Далее индивидуальным клиентским станциям назначается индивидуальные PSK, которые создаются или динамически, или вручную. Как показано на

Рисунок 17.5, несколько PSK пользователь/устройство [multiple per-user/per-device PSKs] могут быть привязаны к одному SSID. Генерированные PSKs также могут иметь дату срока действия. Уникальные PSK с учетом времени [time-based PSKs] могут быть использованы в среде БЛВС как замена более традиционных учетных данных имя пользователя/пароль. В отличие от статических PSKs, PSKs на пользователя/на устройство может обеспечить уникальность идентификационных учетных данных.

**РИСУНОК 17.5** Проприетарный PSK



На текущий момент, четыре производителя корпоративных БЛВС предлагают проприетарные решения аутентификации PSK, которые предоставляют возможность уникального PSK для каждого пользователя или каждого устройства. Это производители Extreme Networks, Cisco, Fortinet, и Ruckus Wireless. Проприетарные решения PSK предоставляют способ внедрения уникальных идентификационных учетных данных без тяжелого развертывания более сложного решения 802.1X/EAP. Атаки социальной инженерии и усиленного перебора по словарю все еще возможны, но их сложнее осуществить, если применены сложные и длинные пароли учетных данных. Если уникальный PSK скомпрометирован, то администратор делает недействительным только учетные данные с PSK одного пользователя, и больше не перенастраивает все точки доступа и устройства конечный пользователей.

Некоторые клиентские устройства БЛВС имеют ограниченную поддержку 802.1X/EAP. В таких ситуациях проприетарные решения PSK могут быть выгодны для такого класса устройств и быть значительно лучше по сравнению со стандартной статической единой аутентификацией PSK. Проприетарное решение PSK обеспечивает уникальные учетные данные пользователей или устройств, которые не может предоставить стандартный PSK. Кроме того, проприетарные решения PSK с уникальными учетными данными не требуют нигде сложной настройки, которая нужна для 802.1X/EAP.

Проприетарные реализации аутентификации PSK не означают замену 802.1X/EAP. Однако, некоторые примеры использования учетных данных PSK для каждого пользователя и каждого устройства набирают популярность на предприятиях. Некоторые из этих примеров использования включают следующее:

### Устаревшие Устройства

Решение индивидуальный PSK на пользователя и на устройство [per-user and per-device PSK solution] может быть использовано, чтобы дополнить безопасность 802.1X/EAP, чтобы обеспечить устаревшие устройства уникальными учетными данными PSK.

### Устройства Сотрудников [BYOD]

Хотя безопасность 802.1X/EAP используется для устройств, принадлежащих

компании, проприетарное применение аутентификации PSK часто используется для безопасности решения использования собственных устройств сотрудников [bring your own device (BYOD)]. Уникальные учетные данные PSK для входа в сеть намного проще, чем поддержка сертификатов для персональных устройств сотрудников.

### Гостевой Доступ

Предоставление уникальных учетных данных PSK для доступа к гостевой БЛВС обеспечивает уникальную идентификацию для каждого гостевого пользователя, а также добавляющий ценность сервис - шифрованного гостевого доступа.

### Устройства IoT

Машины и сенсоры, оснащенные радиомодулями 802.11, часто не поддерживают 802.1X/ EAP. PSK на пользователя и на устройство может обеспечить устройства Интернета Вещей (IoT) уникальными учетными данными аутентификации PSK.

## Одновременная Аутентификация Равных

Поправка 802.11s была принята в 2011 году с целью стандартизации взаимосвязанной сетевой работы [mesh networking] БЛВС 802.11. Сейчас поправка 802.11s является частью стандарта 802.11-2020. Поправка определяла Гибридный Беспроводной Взаимосвязанный Протокол [*Hybrid Wireless Mesh Protocol (HWMP)*], который взаимосвязанные порталы [mesh portals] 802.11 и взаимосвязанные точки доступа [mesh points] могли бы использовать для динамического определения выбора лучшего пути для потока трафика через взаимосвязанный БЛВС [meshed WLAN]. HWMP и другие механизмы, определенные поправкой 802.11s-2011, не были приняты производителями БЛВС из-за конкуренции. Основные производители БЛВС не хотят, чтобы их ТД принимали взаимосвязанную связь [mesh communications] от ТД конкурентов. В результате, основные производители БЛВС предлагают собственные решения по взаимосвязанности [mesh solutions] с использованием своих собственных протоколов взаимосвязанности [mesh protocols] и метрик.

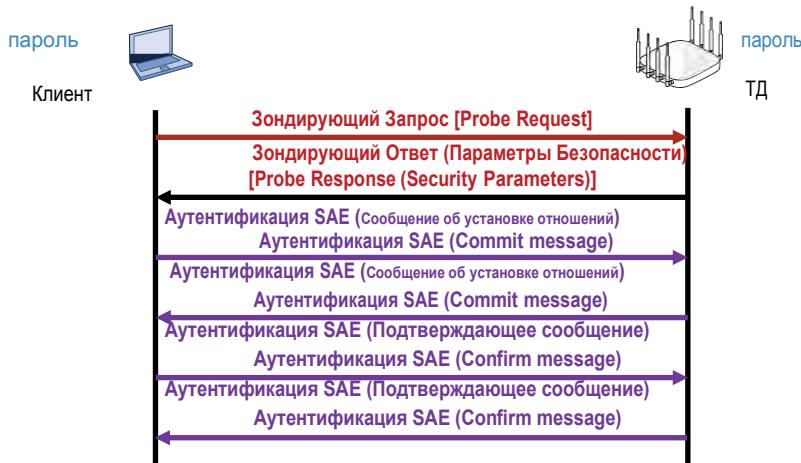
Поправка 802.11s-2011 также определяет методы безопасности RSN, которые могли бы быть использованы взаимосвязанными порталами [mesh portals] и взаимосвязанными точками [mesh points]. *Аутентифицированный Взаимосвязанный Пиринговый Обмен Сообщениями [Authenticated Mesh Peering Exchange (AMPE)]* используется для безопасного создания и обмена парными мастер ключами [pairwise master keys (PMKs)]. 802.1X/EAP мог бы быть одним из методов, используемых для получения PMK во взаимосвязанных [mesh] средах. Этот метод не идеален для взаимосвязанных [mesh] точек, потому что RADIUS сервер находится на проводной сети. Следовательно, поправка 802.11s-2011 предложила новый метод аутентификации равный-с-равным [peer-to-peer], названный *одновременная аутентификация равных [simultaneous authentication of equals (SAE)]*. SAE основан на обмене ключей Дрэгонфлай [Dragonfly key exchange]. Dragonfly в переводе с английского – Стрекоза. Дрэгонфлай [Dragonfly] – это безпатентная и свободная от платежей технология, которая использует обмен ключей с подтверждением с нулевым-знанием [zero-knowledge proof key exchange], что означает, что пользователь или устройство должны подтвердить знание пароля без обязательного раскрытия пароля.

Хотя SAE никогда в действительности не применялся для взаимосвязанных сетей [mesh networks] 802.11, Wi-Fi Альянс рассматривал SAE как будущую замену аутентификации PSK. Как вы уже знаете, аутентификация PSK чувствительна к усиленным атакам перебора по словарю [brute-force dictionary attacks] и очень небезопасна, когда используется слабый, недостаточно надежный пароль. В текущей реализации аутентификации PSK, усиленные атаки перебора по словарю могут быть перехитрены путем использования очень сложного пароля, состоящего от 20 до 63 символов. Атаки перебора по словарю против сложных паролей могут занять годы, прежде чем иметь успех. Однако, атаки по словарю применимы и более легко достижимы путем комбинирования ресурсов распределенных облачных вычислений. Большая озабоченность в том, что большинство пользователей создают только 8-символьный пароль, который обычно может быть скомпрометирован за несколько часов или даже минут. Основная цель SAE – предотвратить все атаки перебора по словарю.

Думайте о SAE как о более безопасном методе аутентификации PSK. Цель в предоставлении того же самого пользовательского опыта, путем продолжения использования пароля. Однако, обмен сообщений протокола SAE защищает пароль от усиленных атак перебора по словарю. Пароли никогда не посылаются между станциями 802.11 во время обмена сообщениями SAE.

Как показано на Рисунке 17.6, процесс SAE состоит из обмена устанавливающими доверительные отношения сообщениями [commitment message exchange] и обмена сообщениями подтверждения [confirmation message exchange]. Доверительный обмен [commitment exchange] используется для принуждения каждого радиомодуля сделать одно предположение о пароле. Далее, используется обмен подтверждениями [confirmation exchange] для подтверждения, что предположение о пароле было корректным. Кадры аутентификации SAE используются для осуществления этих обменов. Пароль используется в SAE, чтобы детерминистически вычислить секретный элемент [secret element] в договаривающейся между собой группе, называемого парольным элементом [password element], который затем используется в аутентификации и протоколе обмена ключами.

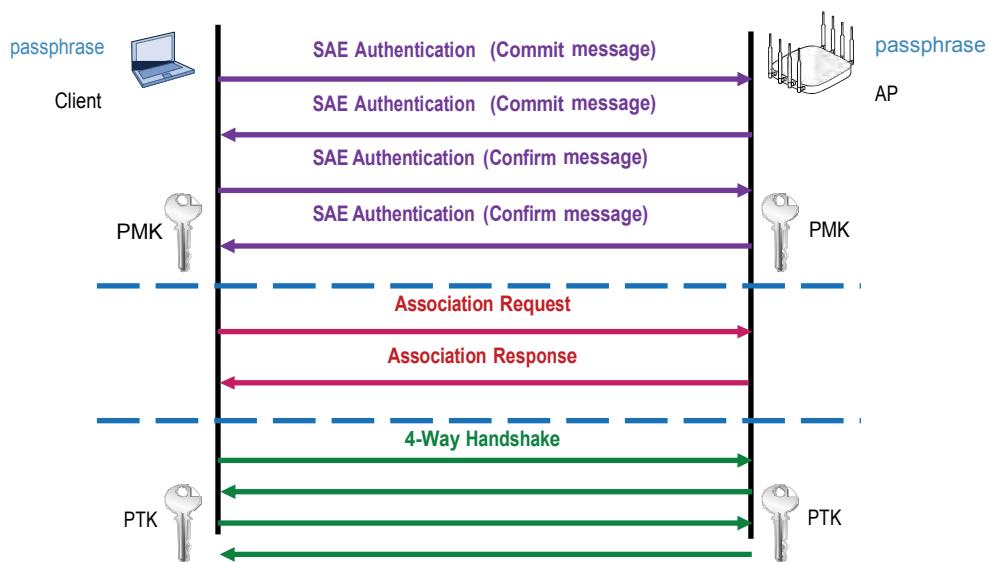
**РИСУНОК 17.6** Обмен сообщениями в аутентификации SAE



Исходное назначение поправки 802.11s было в генерировании парного мастер ключа [pairwise master key (PMK)] из обмена сообщениями SAE, который затем использовался бы для получения временного ключа взаимосвязанности [mesh temporal key (MTK)], чтобы использовать его для шифрования однокомандного [unicast] трафика между взаимосвязанными [mesh] точками доступа. Вместо этого, Wi-Fi Альянс поставил обмен сообщениями SAE между ТД и клиентской станцией для WPA3-Personal. SAE - это замена Wi-Fi Альянсом аутентификации PSK, как часть сертификации безопасности WPA3. Безопасность WPA3 будет обсуждаться более подробно позже в этой главе.

Как изображено на Рисунке 17.7, когда обмен сообщениями SAE завершен, то рассчитан и установлен уникальный парный мастер ключ (PMK) и на ТД 802.11 и на клиентской станции.

PMK является исходным материалом [seeding material] для 4x-Стороннего Рукопожатия, который используется для генерации динамических ключей шифрования. Аутентификация SAE выполняется до ассоциации. Когда PMK создан и процесс ассоциации завершен, то далее ТД и клиент начинают 4x-Стороннее Рукопожатие, чтобы создать парный переходный ключ [pairwise transient key (PTK)]. Подробное объяснение процесса 4x-Стороннего Рукопожатия находится позже в этой главе.

**РИСУНОК 17.7** SAE Аутентификация, ассоциация, ассоциация и 4x-Стороннее Рукопожатие

Как ранее упоминалось, цель SAE решить вопрос с предыдущей слабостью аутентификации PSK. Так как обмен сообщениями SAE разрешает только одно предположение пароля, усиленные оффлайн атаки перебора по словарю больше не жизнеспособны. Атакующий с анализатором протоколов не сможет определить пароль или PMK при прослушивании обмена сообщениями SAE. Дополнительно, обмен сообщениями SAE также устойчив к атакам подделки [forging] и повторов [replay]. Даже если пароль скомпрометирован, он не может быть использован для воссоздания любого ранее созданного PMK.

## УПРАЖНЕНИЕ 17.2

### SAE и Процесс 4x-Стороннего Рукопожатия

- Чтобы выполнить это упражнение, вам нужно сначала загрузить файл SAE.PCAP с веб страницы книги [www.wiley.com/go/cwnasg6e](http://www.wiley.com/go/cwnasg6e).
- После загрузки файла, вам нужна программа по анализу пакетов, чтобы открыть файл. Если у вас еще не установлен анализатор пакетов на компьютере, вы можете загрузить Wireshark с [www.wireshark.org](http://www.wireshark.org).
- С помощью анализатора пакетов откройте файл SAE.PCAP. Большинство анализаторов пакетов показывают список перехваченных кадров в верхнем разделе экрана, с последовательно пронумерованными кадрами в первой колонке.
- Прокрутите вниз список кадров и посмотрите на обмен установочных [commit] и подтверждающих [confirm] сообщений SAE в кадрах с #16 по #24.
- Прокрутите вниз список кадров и посмотрите на обмен сообщениями 4x-Стороннего Рукопожатия, используемого для создания ключей шифрования с кадра #29 по #36.

## Структура 802.1X/EAP

Стандарт IEEE 802.1X это не специальный беспроводной стандарт и часто ошибочно называется как 802.11x. Стандарт 802.1X это стандарт контроля доступа на основе порта [*port-based access control*]. 802.1X-2001 был изначально разработан для сетей 802.3 Ethernet. Позже, 802.1X-2004 обеспечил дополнительную поддержку для беспроводных сетей 802.11 и сетей Волоконно-Оптического Распределенного Интерфейса Данных [Fiber Distributed Data Interface (FDDI)]. Текущая версия стандарта контроля доступа на основе портов 802.1X-2010 определила дальнейшие улучшения. 802.1X обеспечивает авторизационную структуру, которая разрешает или не разрешает трафику проходить через порт, и таким образом иметь доступ к сетевым ресурсам. Структура 802.1X может быть применена и в беспроводной и в проводной средах.

Авторизационная структура 802.1X состоит из трех главных компонентов, каждый из которых со специальной ролью. Эти три компонента 802.1X работают вместе, чтобы гарантировать, что только соответствующим образом подтвержденные пользователи и устройства авторизованы для доступа к сетевым ресурсам. Протокол аутентификации 2ого уровня, называемый Расширяемый Аутентификационный Протокол [Extensible Authentication Protocol (EAP)], используется в структуре 802.1X для подтверждения пользователя на 2ом уровне. Три главных компонента структуры 802.1X:

### Клиент [Supplicant]

Хост с программным обеспечением, который запрашивает аутентификацию и доступ к сетевым ресурсам называется *клиент [supplicant]*. У каждого клиента [supplicant] есть уникальные аутентификационные учетные данные [credentials], которые подтверждаются сервером аутентификации. В БЛВС, клиентом [supplicant] часто является ноутбук или беспроводное ручное устройство, пытающееся получить доступ к сети.

### Аутентификатор [Authenticator]

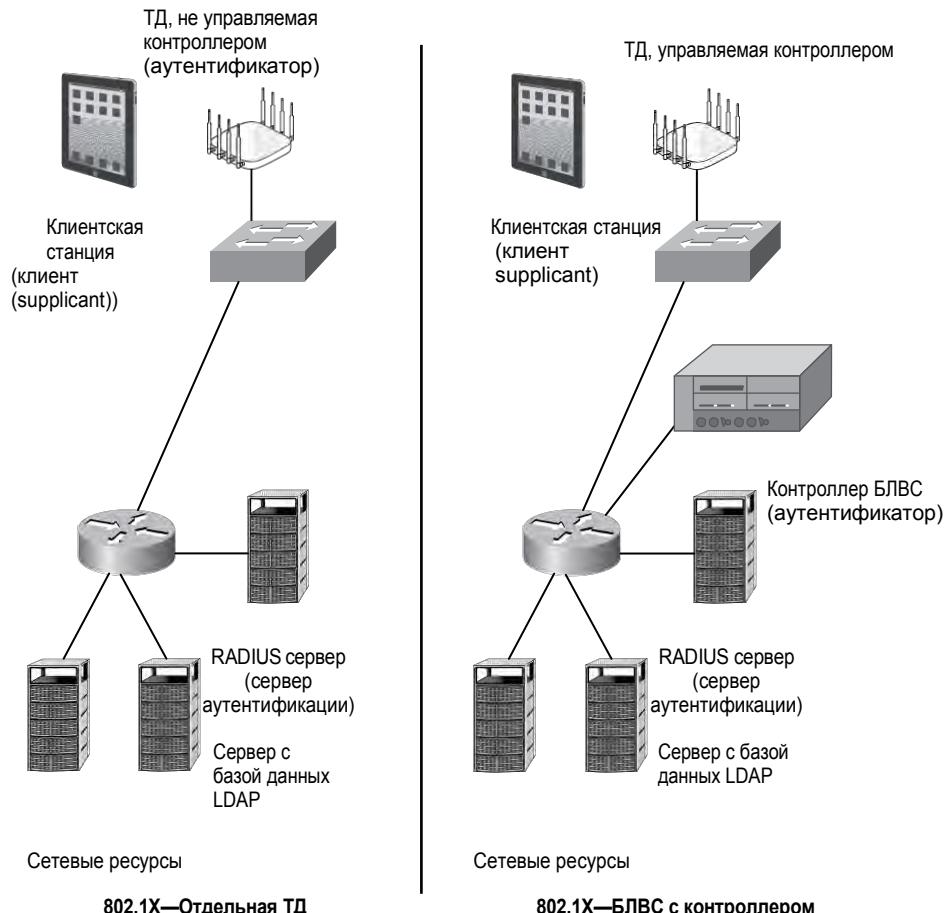
Устройство *аутентификатор [authenticator]* блокирует трафик или разрешает трафику пройти через его порт. Аутентификационному трафику обычно разрешается пройти через аутентификатор, в то время как весь другой трафик блокируется, пока личность клиента [supplicant] не будет подтверждена. Аутентификатор управляет двумя виртуальными портами: *неконтролируемый порт [uncontrolled port]* и *контролируемый порт [controlled port]*. Неконтролируемый порт позволяет трафику аутентификации EAP проходить, в то время как контролируемый порт блокирует весь другой трафик до тех пор, пока клиент [supplicant] не аутентифицируется. В БЛВС аутентификатор - это обычно или ТД или контроллер БЛВС.

### Сервер Аутентификации [Authentication Server]

*Сервер аутентификации [authentication server (AS)]* проверяет верность учетных данных [credentials] клиента [supplicant], который запрашивает доступ и уведомляет аутентификатора, что клиент авторизован. Сервер аутентификации поддерживает свою базу данных или может проксировать запрос во внешнюю базу данных, например в базу данных LDAP, для аутентификации пользовательских учетных данных [supplicant credentials]. RADIUS сервер обычно работает в качестве сервера аутентификации. В сети 802.3 клиентом [supplicant] будет настольный хост (компьютер), аутентификатором будет управляемый коммутатор, а сервером аутентификации обычно бывает сервер Службы Удаленной Аутентификации Пользователей с Телефонным Подключением [Remote Authentication Dial-In User Service] (RADIUS сервер). В беспроводной среде 802.11, клиентом [supplicant] будет клиентская станция, запрашивающая доступ к сетевым ресурсам.

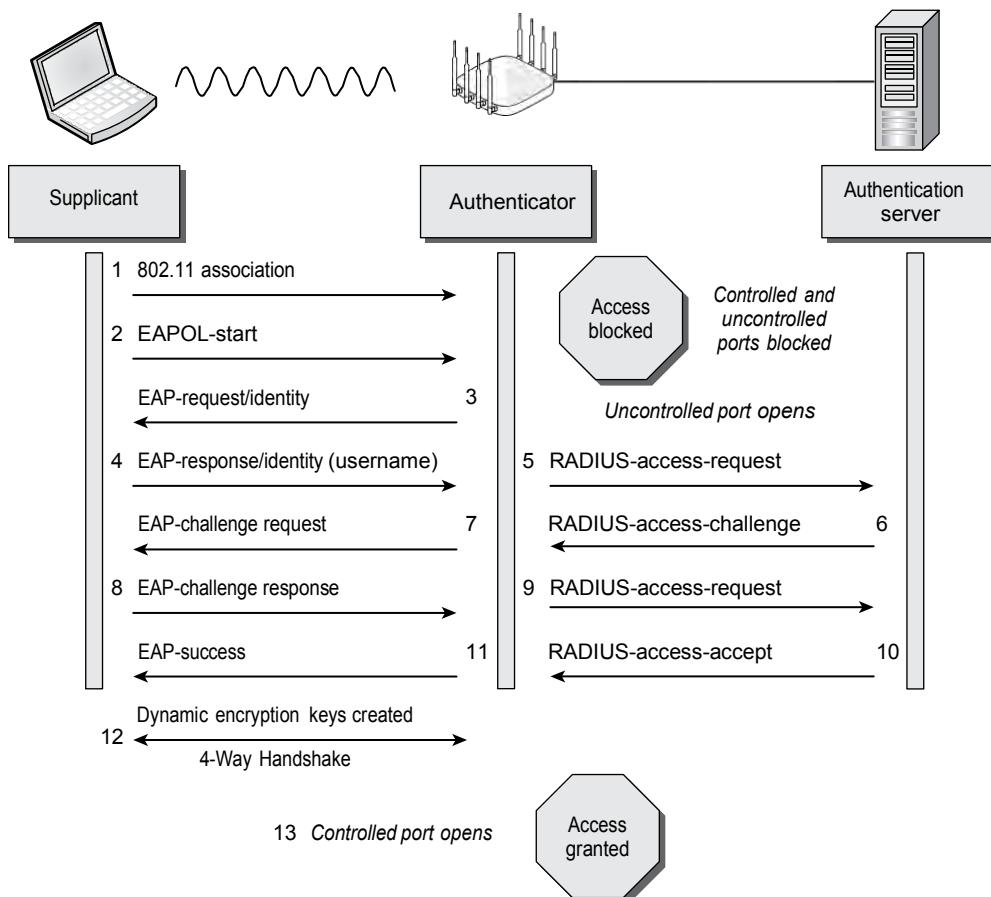
Как показано на Рисунке 17.8, отдельная точка доступа будет аутентификатором, блокирующая доступ через виртуальные порты, а сервером аутентификации обычно является внешний RADIUS сервер. Рисунок 17.8 показывает, что когда решение безопасности 802.1X используется с решением с контроллером БЛВС, то контроллер БЛВС обычно является аутентификатором—а не точки доступа, управляемые контроллером. В любом случае, сервисы каталогов [directory services] часто предоставляются базами данных Облегченного Протокола Доступа к Каталогам [Lightweight Directory Access Protocol (LDAP)], с которыми RADIUS сервер связывается напрямую. Активный Каталог [Active Directory] является примером базы данных LDAP, которая опрашивается RADIUS сервером. Обратите внимание, что некоторые производители БЛВС предлагают решения, где и отдельная ТД, и контроллер БЛВС могут выполнять двойную функцию и как RADIUS сервер и выполнять прямые запросы LDAP, устранив таким образом необходимость во внешнем RADIUS сервере.

**РИСУНОК 17.8** Сравнение 802.1X—отдельная или управляемая контроллером точки доступа



Хотя клиент [supplicant], аутентификатор, и сервер аутентификации работают вместе, чтобы предоставить структуру для контроля доступа на основе портов 802.1X, но нужен протокол аутентификации, чтобы провести процесс аутентификации. Чтобы обеспечить пользовательскую аутентификацию используется *Расширяемый Протокол Аутентификации [Extensible Authentication Protocol (EAP)]*. EAP это гибкий протокол аутентификации 2ого уровня, используемый клиентом и сервером аутентификации для взаимодействия. Аутентификатор позволяет трафику EAP пройти через его виртуальный неконтролируемый порт. После того, как сервер аутентификации подтвердит учетные данные клиента, сервер отправляет сообщение аутентификатору, что клиент [supplicant] аутентифицирован; аутентификатор затем разрешает открыть виртуальный контролируемый порт и разрешает всему другому трафику пройти. Рисунок 17.9 представляет обобщенный обмен кадров 802.1X/EAPs.

**РИСУНОК 17.9** Обмен кадров 802.1X/EAP



Структура 802.1X совместно с EAP предоставляет необходимые средства подтверждения личности пользователя и устройства, а также авторизации клиентской станции для доступа к сетевым ресурсам.

## Типы EAP

Как отмечалось ранее, *EAP* означает *Расширяемый Протокол Аутентификации [Extensible Authentication Protocol]*. Ключевое слово в EAP – *расширяемый [extensible]*. EAP - это протокол 2ого уровня, который очень гибок, и существует много разных модификаций EAP. Некоторые, такие как Облегченный Расширяемый Протокол Аутентификации компании Cisco [Lightweight Extensible Authentication Protocol (LEAP)], являются проприетарными, в то время как другие, как, например, Защищенный Расширяемый Протокол Аутентификации [Protected Extensible Authentication Protocol (PEAP)], считается стандартным. Некоторые предоставляют только одностороннюю аутентификацию; другие предоставляют двустороннюю аутентификацию. Взаимная аутентификация не только требует, чтобы сервер аутентификации подтверждал клиентские учетные данные, но и клиент должен также аутентифицировать законность сервера аутентификации. Подтверждая сервер аутентификации клиент может гарантировать, что имя пользователя и пароль не передан по неосторожности подставному [rogue] серверу аутентификации. Большинство типов EAP, которые требуют взаимную аутентификацию, используют цифровой сертификат на стороне сервера для подтверждения сервера аутентификации. Серверный сертификат устанавливается на RADIUS сервер, в то время как корневой сертификат *центра сертификации (ЦС) [certificate authority (CA) root certificate]* находится на клиенте. Во время обмена сообщениями EAP, клиентский корневой сертификат используется для подтверждения серверного сертификата. Как нарисовано на Рисунке 17.10, обмен сертификатами также создает зашифрованный туннель Уровня Защищенных Сокетов/Безопасности Транспортного Уровня [Secure Sockets Layer (SSL)/Transport Layer Security (TLS)], в котором могут передаваться клиентские учетные данные имя пользователя/пароль или сертификаты. Многие безопасные формы EAP используют *туннелированную аутентификацию [tunneled authentication]*. Туннель SSL/TLS используется для шифрования и защиты пользовательских учетных данных во время обмена сообщениями EAP.

**РИСУНОК 17.10** Туннелированная аутентификация

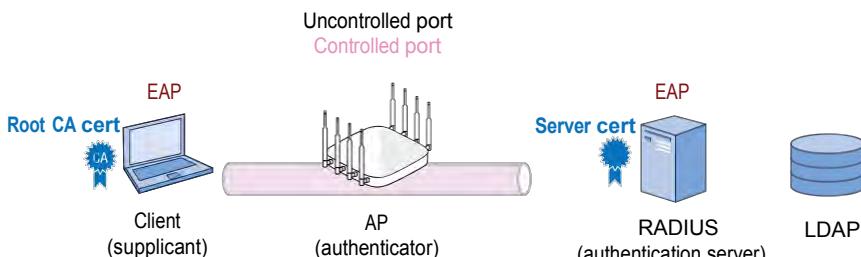


Таблица 17.3 приводит сравнительные данные многих различных типов EAP. Детальное обсуждение всех механизмов аутентификации и различий между различными видами EAP находится за пределами этой книги. Экзамен CWSP усиленно тестирует вас по знанию работы различных типов аутентификации EAP. Экзамен CWNA не тестирует вас на знание определенных функций EAP.

**ТАБЛИЦА 17.3** Сравнительная таблица EAP

|                                | EAP-M05  | EAP-LEAP                            | EAP-TLS  | EAP-ITLS | PEAPv0<br>(EAP-MSCHAPv2) | PEAPv0<br>(EAP-TLS) | PEAPv1<br>(EAP-GTC) | EAP-FAST                     |
|--------------------------------|----------|-------------------------------------|----------|----------|--------------------------|---------------------|---------------------|------------------------------|
| Security Solution              | RFC-3748 | Cisco proprietary                   | RFC-5216 | RFC-5281 | IETF draft               | IETF draft          | IETF draft          | RFC-4851                     |
| Digital Certificates—Client    | No       | No                                  | Yes      | Optional | No                       | Yes                 | Optional            | No                           |
| Digital Certificates—Server    | No       | No                                  | Yes      | Yes      | Yes                      | Yes                 | Yes                 | No                           |
| Client Password Authentication | Yes      | Yes                                 | N/A      | Yes      | Yes                      | No                  | Yes                 | Yes                          |
| PACs-Client                    | No       | No                                  | No       | No       | No                       | No                  | No                  | Yes                          |
| PACs-Server                    | No       | No                                  | No       | No       | No                       | No                  | No                  | Yes                          |
| Credential Security            | Weak     | Weak (depends on password strength) | Strong   | Strong   | Strong                   | Strong              | Strong              | Strong(if Phase 0 is secure) |
| Encryption Key Management      | No       | Yes                                 | Yes      | Yes      | Yes                      | Yes                 | Yes                 | Yes                          |
| Mutual Authentication          | No       | Debatable                           | Yes      | Yes      | Yes                      | Yes                 | Yes                 | Yes                          |
| Tunneled Authentication        | No       | No                                  | Optional | Yes      | Yes                      | Yes                 | Yes                 | Yes                          |
| Wi-Fi Alliance Supported       | No       | No                                  | Yes      | Yes      | Yes                      | No                  | Yes                 | Yes                          |

## Динамическая генерация ключей шифрования

Хотя структура 802.1X не требует шифрования, настойчиво рекомендуется использовать шифрование для обеспечения конфиденциальности данных. Вы уже узнали, что назначение 802.1X/EAP - это аутентификация и авторизация. Если клиент надлежащим образом аутентифицирован сервером аутентификации с помощью протокола EAP 2ого уровня, то клиенту разрешено проходить через контролируемый порт аутентификатора, и связь на высоких уровнях с 3 по 7 для клиента может быть установлена. 802.1X/EAP защищает сетевые ресурсы так, что только подтвержденный клиент авторизован(разрешен) для доступа.

Однако, как показано на Рисунке 17.11, выдающийся побочный продукт 802.1X/EAP - генерация и распространение динамических ключей шифрования. Как ранее упоминалось, динамические ключи шифрования могут быть сгенерированы как побочный продукт аутентификации PSK или SAE. Протоколы EAP, которые используют взаимную аутентификацию предоставляют "исходный материал" [“seeding material”], который может быть использован для создания ключей шифрования динамически. Существует симбиоз между 802.1X/EAP, PSK и аутентификацией SAE, и созданием ключей шифрования. Взаимная аутентификация требуется для генерации уникальных динамических ключей шифрования.

**РИСУНОК 17.11** 802.1X/EAP и динамические ключи



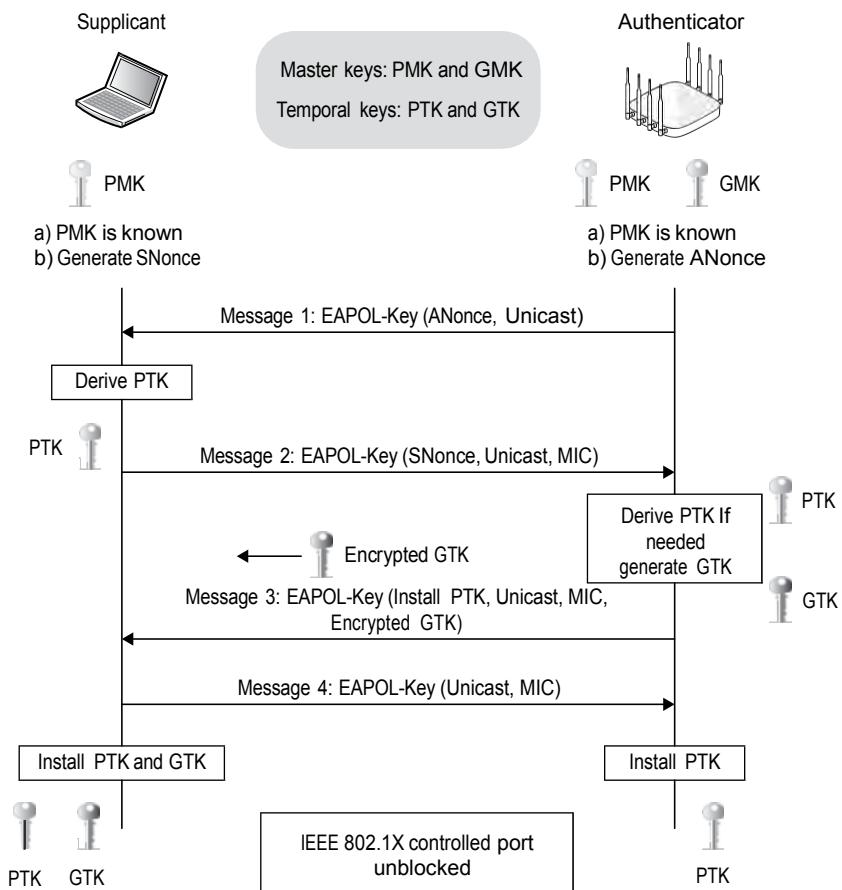
Устаревшая безопасность БЛВС включала использование статических WEP ключей. Использование статических ключей обычно является кошмаром администратора, и когда один и тот же ключ является общим у многих пользователей, статический ключ легко компрометируется с помощью социальной инженерии. Первое преимущество использования динамических ключей по сравнению со статическими в том, что они не могут быть скомпрометированы атакой социальной инженерии, потому что пользователи не знают ключей. Второе преимущество динамических ключей в том, что у каждого пользователя отличающийся и уникальный ключ. Если ключ шифрования одного пользователя будет скомпрометирован, ни один из других пользователей не будет подвергаться риску. Динамически сгенерированные ключи шифрования не делаются общими между пользователями и не известны пользователям.

## 4x-Стороннее Рукопожатие

Как вы только что узнали, существует симбиоз между созданием динамических ключей шифрования и аутентификацией. Парный мастер ключ [pairwise master key (PMK)] используется для проведения [seed] 4x Стороннего Рукопожатия, которое генерирует уникальные динамические ключи, используемыми любыми двумя радиомодулями 802.11. PMK генерируется как побочный продукт или PSK, SAE, или аутентификации 802.1X/EAP.

Как мы объясняли ранее, стандарт 802.11-2020 определяет, что называется надежную безопасную сеть [robust security network (RSN)] и ассоциации надежной безопасной сети [robust security network associations (RSNAs)]. Две станции (STAs) должны установить процедуру для аутентификации и ассоциации друг с другом, а также создать динамические ключи шифрования через процесс, называемый 4x-Стороннее Рукопожатие [*4-Way Handshake*], который изображен на Рисунке 17.12.

**РИСУНОК 17.12** 4x Стороннее Рукопожатие



RSNAs использует способ управления динамическими ключами шифрования, который включает создание пяти отдельных ключей. Полное объяснение процесса находится за пределами этой книги, но короткое объяснение подходит. Часть процесса RSNA включает создание двух мастер ключей, которые называются *групповой мастер ключ* [group master key (GMK)] и *парный мастер ключ* [pairwise master key (PMK)].

Как до этого обсуждалось, существует симбиоз между созданием динамических ключей и аутентификацией. PMK создается в результате аутентификации 802.1X/EAP. PMK может также быть создан из аутентификаций PSK или SAE вместо аутентификации 802.1X/EAP. Эти мастер ключи являются исходным материалом [seeding material], используемым для создания финальных динамических ключей, которые используются для шифрования и расшифровки. Финальные ключи шифрования называются *парный временный ключ* [pairwise transient key (PTK)] и *групповой временный ключ* [group temporal key (GTK)]. PTK используется для шифрования/расшифровки однократного [unicast] трафика, а GTK используется для шифровки/расшифровки широковещательного [broadcast] и многонаправленного [multicast] трафика.

Эти временные ключи создаются во время четырех-стороннего обмена кадрами EAP, которое называется 4x-Стороннее Рукопожатие. 4x-Стороннее Рукопожатие всегда будет финальным четырех кадровым обменом во время 802.1X/EAP, PSK, или SAE аутентификации. Когда бы не создавались динамические ключи TKIP/ARC4 или CCMP/AES, должно происходить 4x-Стороннее Рукопожатие. Также, каждый раз, когда клиентский радиомодуль переключается с одной ТД на другую, должно произойти новое 4x-Стороннее Рукопожатие так, что новые уникальные ключи шифрования могли бы быть сгенерированы. Например, 4x-Стороннее Рукопожатие можно посмотреть в Упражнениях 17.2 и 17.3.



На текущий момент экзамен CWNA не проверяет вас на механику процесса создания динамических ключей шифрования, которая была изначально определена поправкой 802.11i. Процесс генерации динамических ключей шифрования слегка другой, когда применяется 802.11g быстрый BSS переход [fast BSS transition]. Процессы тщательно проверяются на экзамене CWSP.

## УПРАЖНЕНИЕ 17.3

### Процесс 802.1X/EAP и 4x-Стороннего Рукопожатия

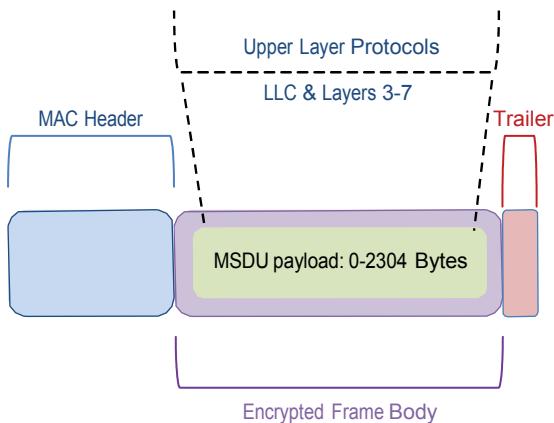
1. Для выполнения этого упражнения вам нужно сначала загрузить файл CWNA CHAPTER17.PCAP с веб-страницы книги [www.wiley.com/go/cwnasg6e](http://www.wiley.com/go/cwnasg6e).
2. После загрузки файла вам нужно программное обеспечение анализа пакетов, чтобы открыть файл. Если у вас еще не установлен анализатор пакетов на вашем компьютере, вы можете загрузить Wireshark с [www.wireshark.org](http://www.wireshark.org).
3. С помощью анализатора пакетов откройте файл CWNA CHAPTER17.PCAP. Большинство анализаторов пакетов показывают список записанных кадров в верхней секции экрана, с последовательно пронумерованными кадрами в первом столбце.
4. Прокрутите вниз список кадров и посмотрите на обмен кадров EAP с кадра #209 до кадра #246.
5. Прокрутите вниз список кадров и посмотрите на 4x-Стороннее Рукопожатие с кадра #247 по кадр #254.

## Шифрование БЛВС

Стандарт 802.11-2020 определяет четыре способа шифрования которые работают на 2м уровне модели OSI: WEP, TKIP, CCMP, и GCMP. Информация, которая защищается методами шифрования 2ого уровня - это данные, находящиеся на верхних уровнях с 3 по 7. Методы шифрования 2ого уровня используются для обеспечения конфиденциальности данных для кадров данных 802.11. Техническое название кадров данных 802.11 - блок данных протокола MAC [*MAC protocol data unit (MPDU)*]. Кадры данных 802.11, как показано на Рисунке 17.13 содержит MAC заголовок 2ого уровня, тело кадра, и окончание, которое является 32-битной проверкой CRC, и которое называется последовательность проверки кадра [*frame check sequence (FCS)*]. Заголовок 2ого уровня содержит MAC адреса и значение длительности [*duration value*].

Инкапсулированное в тело кадра данных 802.11 является полезной нагрузкой верхних уровней, которое называется блок сервисных данных MAC [*MAC service data unit (MSDU)*]. MSDU состоит из данных Контроля Логического Канала Связи [Logical Link Control (LLC)] и уровней 3-7. Простое определение MSDU - это полезная нагрузка данных, которая содержит IP пакет плюс некоторые данные LLC. Когда включено шифрование, полезная нагрузка MSDU в кадре данных 802.11 зашифрована.

**РИСУНОК 17.13** Кадр данных 802.11



WEP, TKIP, CCMP, GCMP, и другие проприетарные методы шифрования на 2ом уровне используются для шифрования полезной нагрузки MSDU кадра данных 802.11.

Следовательно, информация , которая защищается - это верхние уровни 3-7, которые более широко известны как IP пакет [*IP packet*].

Следует отметить, что многие типы кадров 802.11 или никогда не шифруются, или обычно не зашифрованы. Кадры управления 802.11 несут только полезную нагрузку 2ого уровня в своем теле кадра, поэтому шифрование не является необходимым в целях защиты данных. Некоторые кадры управления защищены, если включены механизмы защиты кадров управления 802.11w. MFP обсуждается более детально позже в этой главе. Кадры контроля 802.11 имеют только заголовок и окончание, следовательно шифрование не нужно. Некоторые кадры данных 802.11, такие как пустой кадр действия [*null function frame*], в действительности не имеют полезной нагрузки MSDU . Не неущие

данных кадры имеют специфичную функцию, но они не требуют шифрование. Только кадры данных 802.11 с полезной нагрузкой MSDU могут быть зашифрованы WEP, TKIP, CCMP или GCMP. В рамках корпоративной политики кадры данных 802.11 всегда должны быть зашифрованы в целях конфиденциальности данных и безопасности.

WEP, TKIP, CCMP, и GCMP являются методами шифрования, которые все используют симметричные алгоритмы. WEP и TKIP используют шифр ARC4, когда CCMP и GCMP используют шифр AES. Текущий стандарт 802.11-2020 определяет WEP как устаревший способ шифрования для до-RSNA безопасности. TKIP, CCMP, и GCMP считаются протоколами шифрования надежной защищенной сети [*robust security network (RSN)*]. TKIP не рекомендуется, однако, и GCMP еще не используется на рынке БЛВС предприятий. CCMP является методом шифрования широко используемым для конфиденциальности данных Wi-Fi..

## Шифрование TKIP

Опциональным методом шифрования, определенным для надежной защищенной сети [*robust security network*] является *Протокол Целостности Временного Ключа [Temporal Key Integrity Protocol (TKIP)]*. Этот метод использует шифр ARC4, также как и шифрование WEP. На самом деле TKIP – это расширение шифрования WEP, которое устранило многие из известных уязвимостей WEP. Проблема с WEP была не в шифре ARC4, а в том как создавался ключ шифрования. TKIP была разработана, чтобы устранить проблемы, которые были встроены в WEP.

TKIP стартует с 128-битного временного ключа, который комбинируется с 48-битным вектором инициализации [*initialization vector (IV)*] и MAC адресами источника и назначения в сложном процессе, который называется *смешивание по-пакетных ключей [per-packet key mixing]*. Этот процесс смешивания ключей убирает известные атаки коллизии векторов инициализации [*IV collision*] и слабых ключей против WEP. TKIP также использует последовательный метод [*sequencing method*], чтобы устранить атаки повторной вставки [*reinjection attacks*], используемой против WEP. Кроме того, TKIP использует сильную проверку целостности данных, которая называется *проверка целостности сообщений [message integrity check (MIC)]*, для уменьшения известных атак манипулирования битами [*bit-flipping attacks*] против WEP. MIC иногда называют по прозвищу Майкл [*Michael*]. Все ключи шифрования TKIP являются динамически генерируемые как конечный результат 4x-Стороннего Рукопожатия.

Шифрование WEP добавляет дополнительные 8 байт служебной информации [*overhead*] к телу кадра данных 802.11. Когда применен TKIP, то из-за дополнительной служебной информации из расширенного вектора инициализации [*IV*] и MIC, в итоге добавляется 20 байт служебной информации к телу кадра данных 802.11. Так как TKIP использует шифр ARC4 и является просто WEP, который был улучшен, большинство производителей выпустили обновление прошивки WPA, которая давала устаревшим только-WEP радиомодулям возможность использования шифрования TKIP. Стандарт 802.11-2020 не разрешает использование шифрования WEP или шифрования TKIP для скоростей передачи данных *высокой пропускной способности [high throughput (HT)]* и *очень высокой пропускной способности [very high throughput (VHT)]*. Wi-Fi Альянс будет сертифицировать только радиомодули 802.11n/ac, которые используют шифрование CCMP для более высоких скоростей передачи данных. Для обратной совместимости новые радиомодули будут еще поддерживать TKIP и WEP для более низких скоростей передачи данных, определенных для устаревших радиомодулей

802.11/a/b/g. Хотя и WEP и TKIP определены в стандарте IEEE 802.11-2020, они устарели из-за рисков безопасности и не поддерживаются для скоростей передачи данных 802.11n и 802.11ac. Кроме того, WEP и TKIP не поддерживаются для скоростей передачи данных 802.11ax. WEP и TKIP пока еще остаются опциональными протоколами безопасности, чтобы обеспечить поддержку старых устаревших устройств.



## Пример из Реальной Жизни

### Может ли WEP и TKIP еще использоваться?

Поправки 802.11n и выше не разрешают использование шифрования WEP или шифрование TKIP для скоростей передачи данных высокой пропускной способности [high throughput (HT)], очень высокой пропускной способности [very high throughput (VHT)] или высокой эффективности [high efficiency]. Скорости передачи данных HT введены в 802.11n, скорости передачи данных VHT введены в 802.11ac, а скорости передачи данных HE представлены в 802.11ax. Wi-Fi Альянс сертифицирует 802.11n, 802.11ac, и 802.11ax радиомодули только с использованием шифрования CCMP или GCMP для высоких скоростей передачи данных. Для обратной совместимости новые радиомодули могут пока еще поддерживать TKIP и WEP для более медленных скоростей передачи данных, определенных для устаревших 802.11/a/b/g. WEP и TKIP пока еще остаются опциональными протоколами безопасности для обеспечения поддержки для старых устаревших устройств. Как вы узнали, эти протоколы шифрования устарели и имеют риски по безопасности. Устаревшие клиентские устройства 802.11/a/b/g должны быть заменены, чтобы использовать преимущества более высоких скоростей передачи данных 802.11n/ac/ax и использовать шифрование CCMP/AES. Более того, безопасность WPA3 не поддерживает обратную совместимость для WEP или TKIP.

## Шифрование CCMP

Метод шифрования по умолчанию, определенный в поправке 802.11i, называется *Протокол Режима Счетчика с Кодом Аутентификации из Шифровальных Блоков Цепочки Сообщений* [*Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)*]. Этот метод использует алгоритм Улучшенного Стандарта Шифрования [Advanced Encryption Standard (AES)] (алгоритм Рейндал [Rijndael]). CCMP/AES использует 128-битный размер ключа шифрования и шифрует в 128 битные фиксированной длины блоки. Используется 8-байтная проверка целостности сообщения [message integrity check (MIC)], которая считается намного надежнее, чем та, которая используется в TKIP. Также, из-за надежности шифра AES, не требуется по-пакетное смешивание ключей.

WEP и TKIP используют ARC4, который является потоковым шифром. CCMP использует AES, который является блочным шифром. В отличие от потоковых шифров, которые работают с одним битом в единицу времени, блочный шифр берет фиксированной длины блок открытого текста [plaintext] и генерирует блок шифротекста [ciphertext] такой же длины. Блочный шифр является шифром симметричного ключа, работающего с фиксированной длины группой битов, называемых блоками [blocks]. Например, блочный шифр будет использовать 128-битный блок входного открытого текста [plaintext], а в результате на выходе будет 128 битный блок шифротекста [ciphertext].

Шифрование CCMP/AES назначен Wi-Fi Альянсом для сертификаций WPA2 и WPA3, и был преобладающим методом шифрования БЛВС более 10 лет. Все ключи шифрования

## Шифрование GCMP

Поправка 802.11ad-2012 стандартизовала использование *Протокола Режима Счетчика Галуа [Galois/Counter Mode Protocol (GCMP)]*, который использует криптографию AES. Экстремально высокие скорости передачи данных, определенные 802.11ad, требует GCMP, потому что он более эффективен, чем ССМР. GCMP также рассматривается как optionalный метод шифрования для радиомодулей 802.11ac. ССМР использует 128-битный AES ключ, в то время как GCMP может использовать и 128-битный и 256-битный AES ключ.

GCMP основан на GCM алгоритме шифрования AES. GCM защищает целостность и тела кадров данных 802.11 и выбранных частей заголовка 802.11. Вычисления GCMP могут быть запущены параллельно и являются вычислительно менее интенсивны, чем криптографическая работа ССМР. GCM значительно более эффективнее и быстрее, чем ССМ.

Как и ССМ, GCM использует тот же самый алгоритм шифрования AES, хотя применяется по-другому. GCMP нужна только одна операция AES на блок, сразу же уменьшая процесс шифрования на половину. Дополнительно, GCM не соединяет или не связывает блоки вместе. Так как каждый блок не зависит от предыдущего блока, то они независимы друг от друга и могут быть обработаны одновременно, используя параллельные цепи.

Несколько производителей чипсетов начали предлагать возможности GCMP в некоторых радиомодулях 802.11ax. Дополнительно, Wi-Fi Альянс сейчас определяет optionalный 128-битный режим WPA3-Enterprise, который использует 256-битное GCMP шифрование. GCMP обратно не совместим со старым Wi-Fi оборудованием, и следовательно нужно обновление оборудования и для точек доступа, и для клиентских радиомодулей. Однако, программный клиент может быть использован на клиентской стороне, если клиент может использовать процессор ноутбука для продвинутых вычислений, требуемых 256-битным GCMP.

# Защита Кадров Управления

Некоторые кадры управления являются защищенными, если включены механизмы защиты кадров управления 802.11w [*management frame protection (MFP)*]. 802.11w обеспечивает уровень криптографической защиты для некоторых кадров управления 802.11. 802.11w подразумевает предотвращение некоторых из большинства распространенных атак отказа-в-обслуживании [*denial-of-service (DoS)*] на 2ом уровне, использующие модифицированные кадры управления. Подавляющее большинство устаревших клиентов БЛВС не поддерживают 802.11w и, следовательно, такие функции редко включали на точках доступа. Фактически, использование MFP станет более обычной, потому что это требуется для сертификации безопасности WPA3.

Поправка 802.11w-2009 определяет *надежный кадр управления [robust management frame]* в качестве кадра управления, который может быть защищен сервисом защиты кадров управления [*robust management frames*]. Надежные кадры управления [*robust action frames*], кадры деассоциации [*disassociation*], и кадры деаутентификации. Большая часть кадров действия считается надежной [*robust*], включая кадры действия QoS, кадры действия, блоковые подтверждения [*block ACKs*], и многие другие.

Защита от повторного воспроизведения [*Replay protection*] обеспечивается для надежных кадров управления [*robust management frames*] для STAs, которые используют Протокол Целостности Широковещания/Мультикаста [*Broadcast/Multicast Integrity Protocol (BIP)*]. BIP обеспечивает целостность сообщений и контроль доступа для надежных кадров управления с групповыми адресами. BIP-CMAC-128 обеспечивает целостность данных и защиту от повторного воспроизведения с помощью AES-128 в Режиме CMAC с 128-битным ключом целостности. BIP-CMAC-256 обеспечивает целостность данных и защиту от повторного воспроизведения с помощью AES-256 в Режиме CMAC с 256-битным ключом целостности.

# WPA2

Как вы ранее узнали, сертификация Защищенный Доступ в Wi-Fi 2 [Wi-Fi Protected Access 2 (WPA2)] основан на возможностях надежной защищенной сети [*robust security network (RSN)*], механизмы безопасности, которые изначально были определены в поправке IEEE 802.11i.

Все сертифицированные Wi-Fi WPA2 устройства должны поддерживать методы динамического шифрования CCMP/AES. WPA2 поддерживают обратную совместимость для TKIP и WEP; однако, эти устаревшие методы шифрования устарели и не должны использоваться.

Wi-Fi Альянс определил два метода для авторизации пользователей и устройств в БЛВС. WPA2-Enterprise требует поддержку контроля доступа на основе портов 802.1X для установок на предприятиях. WPA2-Personal использует менее сложный парольный метод, предназначенный для домашнего использования. WPA2-Personal основан на аутентификации PSK. WPA2 имел приемлемый уровень безопасности для Wi-Fi почти 15 лет. В реальном мире большинство установок на предприятиях продолжают использовать WPA2.

# WPA3

В Августе 2019 года Wi-Fi Альянс начал тестирование ТД и клиентов по сертификации *Сертифицированный Wi-Fi WPA3 [Wi-Fi Certified WPA3]*. Защищенный Доступ в Wi-Fi 3 [Wi-Fi Protected Access 3 (WPA3)] определяет улучшения в существующие возможности безопасности WPA2 для радиомодулей 802.11. Он поддерживает новые методы защиты, неразрешая вышедшие из употребления устаревшие протоколы, и требует использование защиты кадров управления [management frame protection (MFP)] для поддержки устойчивости жизненно важных сетей. WPA3-Personal использует одновременную аутентификацию равных [simultaneous authentication of equals (SAE)] для защиты пользователей от атак подбора паролей. WPA3-Enterprise теперь предлагает опциональный эквивалентный 192 битной криптографической надежности.

## WPA3-Personal

Несомненно, самое значимое изменение, определенное WPA3 - это замена аутентификации PSK на аутентификацию SAE, которая устойчива к оффлайн атакам перебора по словарю. WPA3-Personal улучшает безопасность Wi-Fi для домашних пользователей и сред, где 802.1X - не вариант. С точки зрения пользователя, опыт использования при подключении остались теми же самыми. Пароль также используется при подключении; однако, обмен сообщений протокола SAE защищает пароль от усиленных атак перебора по словарю. WPA3-Personal определяет два режима работы:

### WPA3-Personal Only [Только WPA3-Personal]

Этот режим полностью замещает аутентификацию PSK WPA2 и требует использование аутентификации SAE. Этот режим включают на ТД, если все клиенты WPA3-совместимы. Защита кадров управления [Management frame protection (MFP)] требуется для ТД и для клиентов, работающих в этом режиме.

### WPA3-Personal Transition [Переходной WPA3-Personal]

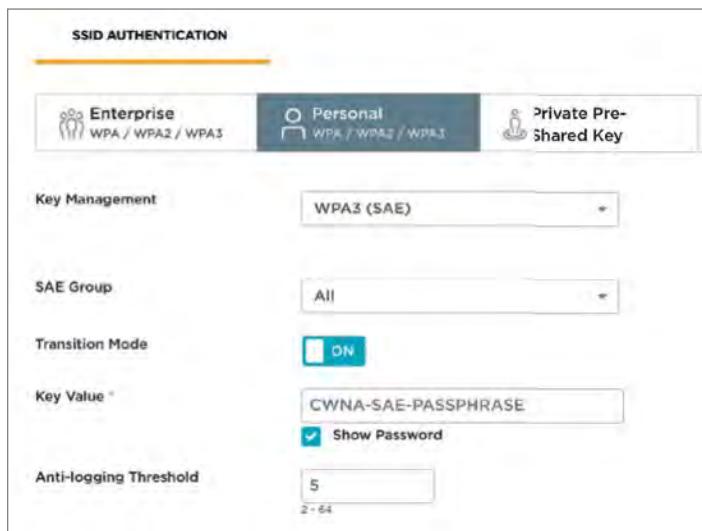
Переходной режим допускает обратную совместимость с WPA2-Personal. Это позволяет клиентам с WPA2-Personal подключиться к тому же самому SSID, что и клиенты WPA3-Personal. Клиенты используют тот же самый пароль; однако, клиенты WPA2 подключаются с аутентификацией PSK, а клиенты WPA3 подключаются с аутентификацией SAE. В этом режиме, MFP используется клиентами WPA3, но не необходимо для клиентов WPA2.

Следующие дополнительные требования применимы к обоим режимам WPA3-Personal:

- Устаревшая безопасность WPA не поддерживается.
- Нет обратной совместимости ни для WEP ни для TKIP.
- Любой клиент WPA3, ассоциированный с ТД, использующий переходный режим WPA3-Personal должен подключаться с SAE.

Как показано на Рисунке 17.14, администраторы имеют возможность выбора включить или выключить переходный режим WPA3-Personal; однако, так как существует очень много клиентов, которые только поддерживают WPA-2 уровень безопасности, переходный режим будет вероятнее всего использоваться очень интенсивно.

**РИСУНОК 17.14** Переходный режим [transition mode] WPA3-Personal



## WPA3-Enterprise

В отличие от WPA3-Personal, где был назначен полностью новый метод аутентификации, WPA3-Enterprise все еще использует 802.1X/EAP для аутентификации корпоративного уровня. Другими словами, процесс аутентификации уровня предприятия остается тем же самым. Двумя основными улучшениями являются поддержка MFP и optionalный улучшенный криптографический режим. WPA3-Enterprise определяет три режима работы:

### WPA3-Enterprise Only [Только WPA3-Enterprise]

Аутентификация 802.1X/EAP остается той же самой. Однако, этот режим будет включен только на ТД, если все клиенты будут WPA3-совместимыми. Защита кадров управления [Management frame protection (MFP)] требуется и для ТД и для клиентов, работающих в этом режиме.

### WPA3-Enterprise Transition [Переходный WPA3-Enterprise]

Переходный режим допускает обратную совместимость с WPA2-Enterprise.

Это позволяет клиентам с WPA2-Enterprise подключаться к тому же самому SSID, что и клиентам с WPA3-Enterprise. Аутентификация 802.1X/EAP остаётся той же самой. Однако, в этом режиме MFP используется клиентами с WPA3, но необязательна для клиентов с WPA2.

### WPA3-Enterprise 192-Bit

Этот режим может быть развернут в чувствительных корпоративных средах для дальнейшей защиты Wi-Fi сетей с более высокими требованиями по безопасности такими как правительственные, оборонные и промышленные среды. Это опциональный режим [*optional mode*], использующий протоколы безопасности с минимальной надежностью в 192 бита и криптографическими инструментами для лучшей защиты чувствительных данных. Некоторые требования режима WPA3-Enterprise 192-bit включают:

- 256-битный GCMP/AES используемый для шифрования кадров данных, а не стандартный CCMP/AES с 128-битным шифрованием.
- Требуется защита кадров управления [Management frame protection (MFP)].
- Используется 256-битный Широковещательный/Многонаправленный Протокол Целостности Кода Галуа Сообщений Аутентификации [256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256)] для защиты кадров управления, а не обычный согласуемый BIP-CMAC-128.
- В качестве протокола аутентификации используется EAP-TLS.

Следующие дополнительные требования применяются ко всем режимам WPA3-Enterprise:

- Устаревшая безопасность WPA не поддерживается.
- Нет поддержки обратной совместимости ни для WEP, ни для TKIP.

Еще один компонент WPA3 это поддержка *быстрого BSS перехода* [*fast BSS transition (FT)*], также называемого как механизм быстрого безопасного роуминга 802.11r. Функции FT сертифицировали в прошлом как часть сертификации Wi-Fi Альянса Голос для Предприятий [Wi-Fi Alliance's Voice Enterprise]. Поскольку механизмы FT напрямую связаны с безопасностью, то FT теперь является опциональным сертификационным компонентом для всех Wi-Fi СЕРТИФИЦИРОВАННЫХ WPA3 [Wi-Fi CERTI-FIED WPA3] устройств.

Постарайтесь думать о сертификации безопасности WPA3 как о постоянной работе в процессе выполнения. Недавнее обновление WPA3-Enterprise включает проверку серверного сертификата для клиентов, использующих EAP-TTLS, EAP-TLS, EAP-PEAPv0, и EAP-PEAPv1 методы. Проверка серверного сертификата WPA3-Enterprise требует, чтобы клиентское устройство подтвердило сертификат RADIUS сервера до получения доступа к сети. Подтверждение корректного RADIUS сервера в сети WPA3-Enterprise может помочь предотвратить атаки человек-по-середине [*man-in-the-middle*].

На момент написания, некоторые другие будущие улучшения безопасности WPA3 включают следующее:

- *Защита маяка* [*Beacon protection*]—Аналогично MFP, защит маяка предотвращает манипуляцию с кадрами маяками.
- *Подтверждение ТД* [*AP validation*] разработано для публичных сетей, и механизмы

доступны для предотвращения атак типа злой двойник [evil twin].

- *Подтверждение работающего канала [Operating channel validation]* - это безопасный способ подтверждения оповещений о переключении канала [channel switch announcements (CSAs)].
- *Индикации выключения перехода [Transition disable indications]* являются механизмами, используемыми для предотвращения атак на понижение уровня [downgrade attacks] нацеленных на переходные WPA3 режимы.
- Был улучшен SAE.



### Уязвимости Переходного WPA3 Режима

Поймите, что, когда вы используете переходный режим WPA3, вы также наследуете старые уязвимости. Например, переходной режим WPA3-Personal вероятно будет интенсивно использоваться чтобы разрешить обратную совместимость с устройствами WPA2-Personal. Однако, устройства WPA2-Personal все еще чувствительны к усиленным оффлайн атакам перебора по словарю. Пароль все еще может быть скомпрометирован опытным атакующим, ищущим получить незаконный доступ. Кроме того, использование переходных режимов WPA3-Personal и WPA3-Enterprise означает, что устаревшие клиенты вероятно не используют защиту кадров управления.

Пожалуйста, понимайте, что безопасность WPA2 не сломана. Пароль WPA2-Personal сложно взломать, если вы следуете передовому опыту Wi-Fi Альянса по использованию надежного пароля (смесь буквенно-цифровых и пунктуационных знаков, смешанный регистр, 20 и более символов). Однако, большинство домашних пользователей не следуют этому передовому опыту, поэтому WPA3-Personal с аутентификацией SAE является заведомо лучшим вариантом.

Несмотря на переходные режимы, предлагаемые WPA3, текущие тактические развертывания безопасности WPA3 редки на предприятиях. WPA2-Enterprise все еще предлагает почти тот же самый уровень аутентификационной 802.1X/EAP безопасности как и WPA3-Enterprise. Огромная часть парка корпоративных Wi-Fi клиентов поддерживает и продолжает использовать безопасность WPA2. Даже хотя возможно обновление прошивки WPA3 для старых клиентских устройств, основные производители клиентов могут никогда не предложить обновление прошивки до WPA3 для клиентских устройств, которым три и более лет. Однако, Wi-Fi Альянс обязывает поддерживать безопасность WPA3 для сертификации Wi-Fi 6, что означает, что все радиомодули 802.11ax должны поддерживать WPA3. Более того на 1июля 2020года Wi-Fi Альянс обязывает поддерживать WPA3 для всех будущих сертификаций.

## Улучшенная Открытость

Традиционно, Wi-Fi хотспоты и гостевые БЛВС принуждают вас использовать открытую безопасность без шифрования или аутентификации. Сертификация СЕРТИФИЦИРОВАННЫЙ Wi-Fi Улучшенной Открытости [Wi-Fi CERTIFIED Enhanced Open] определяет улучшенную конфиденциальность данных в открытых Wi-Fi сетях. Эта сертификация основана на протоколе Гибкого Беспроводного Шифрования

[*Opportunistic Wireless Encryption (OWE)*]. OWE определяется в IETF RFC 8110.

Протокол OWE интегрирует установленные механизмы криптографии для обеспечения каждого пользователя уникальным индивидуальным шифрованием, защищающим обмен данных между пользователем и точкой доступа. Пользовательский опыт остается тем же самым, что и с открытой безопасностью, потому что не нужно вводить пароль до присоединения к сети. Атаки злонамеренного прослушивания устраниются, потому что кадры данных 802.11 зашифрованы, но нет аутентификационной безопасности.

Улучшенная Открытость [Enhanced Open] не является частью WPA3 и полностью другая и опциональная сертификация безопасности. Существует два режима работы OWE:

#### **Только Улучшенная Открытость [Enhanced Open Only]**

Этот режим использует протокол OWE для обеспечения 128-битного CCMP/AES шифрования для конфиденциальности данных. Кадры данных 802.11 зашифрованы, и также требуется защита кадров управления. Не используется никакой протокол аутентификации.

#### **Переходная Улучшенная Открытость [Enhanced Open Transition]**

Этот режим обеспечивает обратную совместимость с массой клиентов, которые не поддерживают OWE с помощью использования двух SSIDs. Когда настраивается открытый SSID на Улучшенную Открытость [Enhanced Open] на сертифицированной ТД, автоматически создается второй скрытый SSID, который использует OWE.

Устаревшие клиенты подключаются к открытому SSID без шифрования. Однако, внутри кадра-маяк открытого SSID есть информационный элемент OWE, который направляет клиентов Улучшенной Открытости [Enhanced Open] на скрытый SSID, который использует OWE. OWE SSID скрыт, чтобы избежать путаницы для драйверов устаревших клиентов.

Вы должны понимать, что Улучшенная Открытость [Enhanced Open] соответствует только половине требования всесторонней безопасности Wi-Fi. OWE обеспечивает шифрование и конфиденциальность данных, но нет никакой аутентификации. Как недавно упомянули, Улучшенная Открытость [Enhanced Open] -это опциональная, т.е. необязательная сертификация по безопасности. В результате, многие производители БЛВС все еще не поддерживают OWE, а поддержка с клиентской стороны в лучшем случае минимальна. Следовательно, тактическое развертывание OWE на текущий момент редкое явление. Однако, когда 6ГГц ТД и клиенты появятся в 2021, должны будут поддерживать OWE и Улучшенную Открытость [Enhanced Open] для сертификации Wi-Fi 6E.



#### **Пример из Реальной Жизни**

##### **Является ли Улучшенная Открытость [Enhanced Open] лучшим вариантом для Публичных Wi-Fi Хотспотов?**

Публичные хотспоты Wi-Fi традиционно используют открытые сети с минимальной или отсутствующей безопасностью. Хотя OWE может казаться лучшим вариантом для публичного Wi-Fi, намного более защищенная альтернатива - это публичный доступ через технологию Хотспот 2.0 [Hotspot 2.0]. Главная цель Хотспот 2.0 [Hotspot 2.0] это сделать публичные/коммерческие Wi-Fi сети такими же безопасными как и Wi-Fi сети на предприятиях и простоту использования как у домашних Wi-Fi сетей. Пасспоинт [Passpoint] - это бренд сертификационной программы, управляемой Wi-Fi Альянсом. Сертификация Passpoint основана на спецификации Hotspot 2.0 Wi-Fi Альянса. Очень подробное обсуждение о Hotspot 2.0 и Passpoint можно найти в Главе 18

"Оборудование сотрудников (BYOD) и Гостевой доступ".

## Безопасность Wi-Fi 6 ГГц

Вы также должны принять во внимание Wi-Fi безопасность при развертывании Wi-Fi в полосе частот 6 ГГц. Wi-Fi Альянс требует сертификацию по безопасности WPA3 для устройств Wi-Fi 6E, которые работают в полосе 6 ГГц.

Однако, не будет никакой поддержки обратной совместимости для безопасности WPA2. Более того, сертификация Улучшенной Открытости [Enhanced Open], использующая OWE, также будет обязательна.

В результате можно сделать несколько ключевых выводов о 6 ГГц:

- Так как поддержка OWE будет обязательной, то не будет никаких SSID "открытой" безопасности, работающих в 6 ГГц. OWE обеспечивает шифрование без аутентификации. Это может иметь некоторые последствия для SSID гостевого доступа. Неважно какой вариант лучше WPA3-Personal или WPA3- Enterprise, так как аутентификация также является требованием.
- Так как нет обратной совместимости для WPA2, то не будет поддержки аутентификации PSK. Замена аутентификации PSK в WPA3-Personal -это одновременная аутентификация равных (SAE). WPA3-Enterprise продолжит использовать 802.1X. Защита кадров управления(MFP) также будет требоваться.
- Так как нет обратной совместимости для WPA2, то не будет необходимости в переходном режиме WPA3-Personal и переходном режиме WPA3-Enterprise.
- Так как существующие 15 миллиардов клиентов никогда не смогут подключиться в 6 ГГц, видится вероятным, что будут использоваться разные уровни безопасности в разных полосах частот. WPA3 будет использоваться в 6 ГГц, WPA2 останется преобладающим в полосах 2,4 ГГц и 5 ГГц еще долгое время. Однако, прогнозируемое принятие установок 6 ГГц может также ускорить переход на безопасность WPA3 в других полосах частот.

## Сегментация Трафика

Как ранее обсуждалось в этой главе, сегментация является ключевой частью сетевого дизайна. Авторизовавшись (т.е. получив доступ) к сетевым ресурсам, пользовательский трафик может быть дальше ограничен как по тому к каким ресурсам у него может быть доступ, так и куда пользовательский трафик может быть направлен. Сегментация может быть достигнута различными средствами, включая межсетевые экраны, маршрутизаторы, VPNы, и VLANы. Общая стратегия беспроводной сегментации, используемая в корпоративных БЛВС 802.11 - это сегментация на Зем уровне, которая применяет привязку VLANов к различным подсетям. Сегментация также часто переплетена с контролем доступа на основе ролей [role-based access control ] (RBAC).

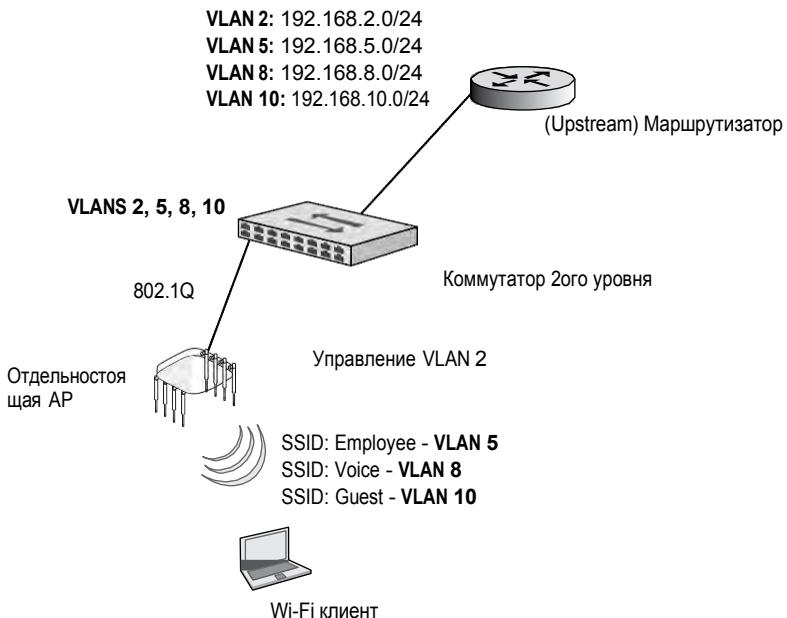
## VLANs

*Виртуальные Локальные Вычислительные Сети [Virtual local area networks (VLANs)]* используются для создания отдельных широковещательных доменов в сетях 2ого уровня, и часто используются для ограничения доступа к сетевым ресурсам не зависимо от физической топологии сети. VLANы являются концепцией 2ого уровня и используются интенсивно в коммутируемых сетях 802.3 в целях безопасности и сегментации. VLANам ставятся в соответствие уникальные подсети 3его уровня, хотя возможно попадание в VLAN нескольких подсетей. VLANы используются для поддержки нескольких сетей 3его уровня на одном и том же коммутаторе 2ого уровня.

Как вы узнали в Главе 11 "Архитектура БЛВС", где используются VLANы в срезе БЛВС зависит от дизайна сети, а также от типа применяемой архитектуры БЛВС. Одна очень большая разница между использованием централизованной пересылкой данных по сравнению с распределенной пересылкой данных в том, как применяются VLANы в сетевом дизайне. В модели с контроллером БЛВС, большая часть пользовательского трафика пересыпается в центр к контроллеру от ТД. Пользовательские VLANы все еще доступны беспроводным пользователям, потому что все пользовательские VLANы инкапсулированы в IP туннель между ТД, управляемой контроллером, на границе и контроллером БЛВС в ядре.

Проект распределенной пересылки данных, однако, требует поддержку нескольких пользовательских VLANов на границе. Каждая точка доступа, таким образом, подключается к транковому порту 802.1Q пограничного коммутатора, который поддерживает разметку VLANов. Все пользовательские VLANы настраиваются на коммутаторе уровня доступа. Точки доступа подключаются к транковому порту 802.1Q пограничного коммутатора. Пользовательские VLANы помечаются метками в транке 802.1Q, и весь беспроводной пользовательский трафик пересыпается на границе сети.

В среде БЛВС индивидуальные SSID могут быть связаны с индивидуальными VLANами, и пользователи могут быть сегментированы по парам SSID/VLAN, при этом все осуществляют связь через одну точку доступа. Каждый SSID также может быть настроен с отдельными настройками безопасности. Большинство корпоративных точек доступа могут вешать несколько SSID, и каждый SSID может быть привязан к уникальному VLANу. Общая стратегия - это создание пар SSID/VLAN для гостей, для голоса и для сотрудников, как показано на Рисунке 17.15. Доступ к управлению контроллеров БЛВС или ТД должен быть изолирован в отдельном VLANe.

**РИСУНОК 17.15** Беспроводные VLANы

### Гостевой SSID/VLAN

SSID, привязанный к гостевому VLANy, часто является открытым, хотя все гостевые пользователи должны быть ограничены политиками межсетевого экрана. Гостевым пользователям запрещен доступ к локальным сетевым ресурсам и они маршрутизируются в Интернет шлюз.

### Голосовой SSID/VLAN

Голосовой SSID может использовать решение по безопасности, такое как пароль в WPA2, и клиентский VoWiFi трафик обычно маршрутизируется на VoIP сервер или учрежденческую автоматическую телефонную станцию (УАТС) [private branch exchange (PBX)].

### SSID/VLAN Сотрудников

SSID для сотрудников использует более сильное решение безопасности, такое как WPA2-Enterprise и списки контроля доступа [access control lists (ACLs)] или политики межсетевого экрана, разрешая сотрудникам полный доступ к сетевым ресурсам после аутентификации.

Большинство производителей БЛВС позволяют радиомодулю вещать до 16 SSID. Однако, вещание 16 SSID - это плохая практика, из-за служебной информации 2ого уровня [overhead], создаваемый кадрами управления и контроля 802.11 для каждого SSID. Вещание 16 SSID приведет к деградации производительности. Передовой опыт в том, чтобы никогда не вещать более трех или четырех SSID.

Что, если вы хотите, чтобы ваши сотрудники были сегментированы на несколько VLANов? Может ли один SSID сотрудников быть связан с несколькими VLANами? RADIUS атрибуты могут быть использованы для присвоения VLANa, когда используется аутентификация 802.1X/EAP на SSID для сотрудников. Как вы уже знаете, когда RADIUS сервер предоставляет успешный ответ на запрос аутентификации, ответ Access-Accept может содержать серию *пар атрибут-значение [attribute-value pairs (AVPs)]*. Одно из наиболее популярных использований RADIUS AVPs - это распределение пользователей по VLANам, на основе их идентификации по пользовательской аутентификации. Вместо сегментации пользователей по разным SSID, которые связаны с уникальными пользовательскими VLANами, все пользователи могут быть ассоциированы с одним SSID и назначены разным VLANам. RADIUS сервер может быть настроен с разными политиками доступа для разных групп пользователей. Политики доступа RADIUSа обычно связывают с разными группами LDAP.

## RBAC

Использование RADIUS-атрибутов для назначения VLANов пользователям была стратегией сетевого дизайна многие годы. Однако, RADIUS атрибуты могут быть далее применены для назначения разным группам пользователей всевозможные виды разных настроек пользовательского трафика, включая VLANы, политики межсетевого экрана, и многое другое.

*Контроль доступа на основе ролей [Role-based access control (RBAC)]* является подходом к ограничению доступа к системе авторизованным пользователям. Основные решения производителей корпоративных БЛВС имеют функционал RBAC. Три главные компоненты подхода RBAC это пользователи [users], роли [roles] и разрешения [permissions]. Могут быть созданы отдельные роли, такие как роль продавцов или роль маркетинга. Разрешения пользовательского трафика могут быть определены как разрешения на 2ом уровне (MAC фильтры), VLANы, разрешения Зего уровня (списки контроля доступа [access control lists]), разрешения уровней 4–7 (межсетевые правила с учетом состояния сессии [stateful firewall rules]), и разрешения по полосе.

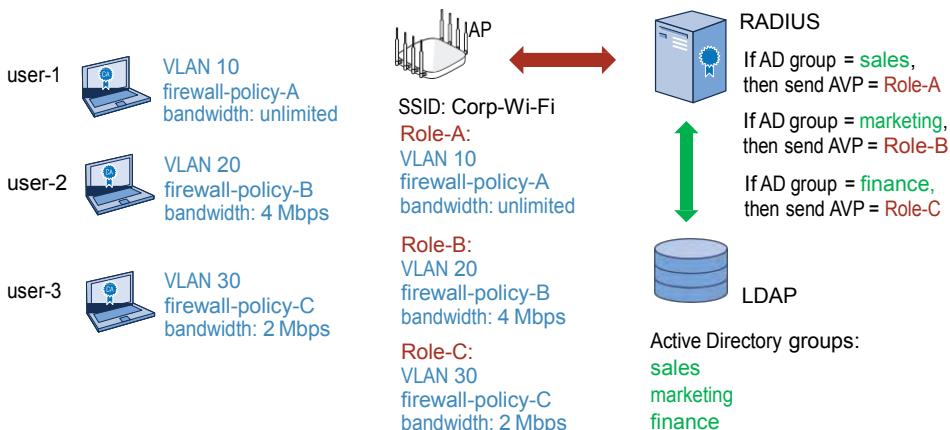
Все эти разрешения также могут быть на основе расписания по времени. Разрешения пользовательского трафика привязываются к ролям. Некоторые производители БЛВС используют термин “роли”, когда другие производители используют термин “пользовательские профили” [“user profiles.”]

Когда пользователь аутентифицируется с помощью 802.1X/EAP, пары атрибут-значение RADIUSa [RADIUS attribute value pairs (AVPs)] могут быть использованы для назначения пользователям определенных ролей автоматически. Все пользователи могут ассоциироваться с одним и тем же SSID, но им могут быть назначены уникальные роли. Этот метод часто используется для назначения пользователям из

определенных групп *Активного Каталога* [Active Directory (AD)] предопределенные роли, созданные на контроллере БЛВС или точке доступа. Каждая роль имеет уникальные ограничения доступа. Когда пользователям назначены роли, они сохраняют разрешения пользовательского трафика какие бы роли им не назначали.

Рисунок 17.16 изображает RADIUS сервер с тремя уникальными политиками доступа привязанных к трем разным группам Активного Каталога [Active Directory]. Например, пользователь-2 [user-2] принадлежит группе маркетинг [marketing] в AD. На основе политик доступа RADIUSa для этой группы AD, когда пользователь-2 [user-2] аутентифицируется, RADIUS сервер пошлет ТД RADIUS пакет с атрибутами, который содержит значение, соответствующее Роли-Б [Role-B], которая настроена на ТД. Клиенту БЛВС пользователь-2 [user-2] будет назначен VLAN 20, политика Б межсетевого экрана [firewall-policy-B], и политика по полосе в 4 Мбит/с.

**РИСУНОК 17.16** RADIUS атрибуты для назначения роли



## Беспроводная безопасность с VPN

Хотя стандарт 802.11-2020 четко определяет решения безопасности на 2ом уровне, решения *виртуальной частной сети* [virtual private network (VPN)] верхнего уровня также могут быть развернуты в БЛВС. VPNы обычно не рекомендуются для обеспечения беспроводной безопасности на предприятиях из-за дополнительной служебной информации [overhead] и потому, что теперь доступны более быстрые, более безопасные решения 2ого уровня. Хотя обычно это не рекомендованная практика, VPNы часто использовались для безопасности БЛВС, так как решение VPN уже было внутри проводной инфраструктуры— особенно в то время, когда WEP был взломан и доказана его небезопасность. VPNы имеют свое место в безопасности Wi-Fi и должны определенно использоваться для удаленного доступа. Они иногда также используются в беспроводных мостах. Два главных типа VPN топологий – это маршрутизатор-маршрутизатор и клиент-сервер.

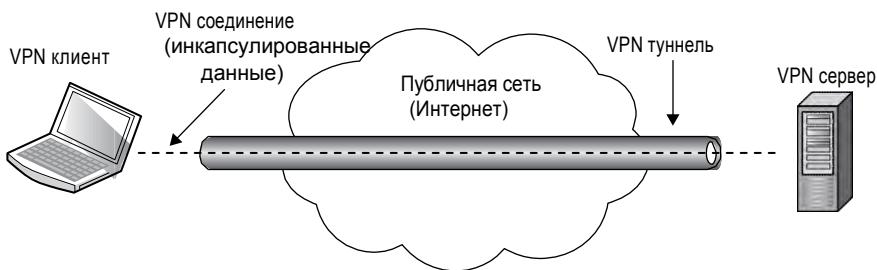
Использование технологии VPN обязательно для удаленного доступа. Ваши сотрудники забирают с собой свои ноутбуки и вероятнее всего используют публично доступные Wi-Fi хотспоты. Большая часть БЛВС публичного доступа не обеспечивает безопасность, поэтому нужно решение по VPN. Пользователю VPN нужно будет

принести безопасность в хотспот, чтобы обеспечить безопасное шифрованное соединение. Крайне важно, чтобы пользователи применяли решение VPN в паре с персональным межсетевым экраном [firewall] всегда, когда получают доступ к любым публичным Wi-Fi сетям. Даже если публичный хотспот предлагает некоторый уровень безопасности, такой как OWE или Passpoint, корпоративная политика может продолжать требовать использование VPN решения компании.

## Просто VPN

Прежде чем обсуждать способы, которыми используются VPN в БЛВС, важно рассмотреть, что же такое VPN, что он делает, как он работает, и компоненты, которые настраиваются, чтобы его построить. Теперь вы знаете, что VPN – это виртуальная частная сеть. Но что это в действительности означает? Как показано на Рисунке 17.17, VPN – это, фактически, частная сеть, которая создается или растягивается через публичную сеть. Для того, что VPN работал, два компьютера или устройства связываются, чтобы установить, что называется VPN туннель [*VPN tunnel*]. Обычно, VPN клиент инициирует соединение пытаясь связаться с VPN сервером.

**РИСУНОК 17.17** Компоненты VPN



VPN клиент может быть компьютером, маршрутизатором, контроллером БЛВС или даже ТД, как вы узнаете позже в этой главе. Когда клиент и сервер могут связаться друг с другом, клиент попытается аутентифицироваться на сервере, путем отправки ему своих учетных данных – [credentials]. Сервер берёт клиентские учетные данные и проверяет их действительность, т.е. валидирует их. Если клиентские учетные данные подтверждены (или действительны), то сервер и клиент создают VPN туннель между собой. Любые данные, которые посылаются от VPN клиента на VPN сервер инкапсулируются в VPN туннель. Клиент и сервер также согласовывают будут ли и как шифроваться данные. Прежде чем данные будут инкапсулированы в туннель, данные шифруются, чтобы гарантировать, что они не смогут быть скомпрометированы пока проходят через туннель. Поскольку нижележащее основание VPN это данные, идущие через небезопасную публичную сеть, безопасность является одной из основных причин по применению VPN.

Когда клиент и сервер строят туннель, то это их ответственность маршрутизировать данные через публичную сеть между двумя устройствами. Они берут данные из локальной сети, шифруют и инкапсулируют их, и затем отправляют на другое устройство, где декапсулируют и дешифруют, и затем помещают в локальную сеть другого устройства.

## VPNы Зего Уровня

У VPНов есть несколько главных характеристик. Они обеспечивают шифрование, инкапсуляцию, аутентификацию, и целостность данных. VPNы используют безопасное туннелирование [*secure tunneling*], которое является процессом инкапсуляции одного IP пакета в другой IP пакет. Первый пакет инкапсулируется во второй, или внешний пакет. Исходные IP адреса назначения и источника первого пакета шифруются вместе с данными полезной нагрузки первого пакета. Следовательно, VPN туннелирование защищает ваши исходные частные адреса Зего уровня, а также защищают данные полезной нагрузки исходного пакета. VPNы Зего уровня используют шифрование Зего уровня; следовательно, полезная нагрузка, которая шифруется, является информацией уровней 4-7. IP адреса второго или внешнего пакета видны открытым текстом и используются для связи между конечными точками туннеля. IP адреса назначения и источника второго или внешнего пакета будут указывать публичные IP адреса VPN сервера и VPN клиента.

Самая широко используемая технология VPN Зего уровня это *Безопасность Интернет Протокола [Internet Protocol Security (IPsec)]*. IPsec VPNы используют более сильные методы шифрования и более безопасные методы аутентификации и являются наиболее широко развернутыми решениями VPN. IPsec поддерживает несколько шифров, включая DES, 3DES, и AES. Аутентификация устройств достигается с помощью или серверного сертификата, или предварительно известного общего ключа [*preshared key*]. Большинство IPsec VPNов являются пересекающими NAT [*NAT-transversal*], но от любых межсетевых экранов на удаленных местах требуется (как минимум), чтобы порты UDP 4500 и 500 были открыты. Полное объяснение технологии IPsec находится за пределами этой книги, но IPsec обычно является выбором VPN технологии на предприятиях.

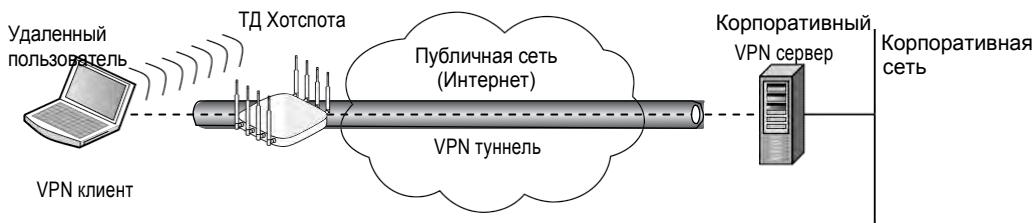
## SSL VPNs

Существуют VPN технологии, которые работают на других уровнях модели OSI, включая SSL туннелирование. В отличие от IPsec VPN, SSL VPN не нужна установка и настройка программного клиента на компьютере конечного пользователя. Пользователь может подключиться к серверу VPN Уровня Безопасных Сокетов [*Secure Sockets Layer (SSL)*] через веб браузер. Трафик между веб браузером и SSL VPN сервером шифруется протоколом SSL или Безопасностью Транспортного Уровня [*Transport Layer Security*] (TLS). TLS и SSL шифруют соединения данных поверх Транспортного уровня с помощью асимметричной криптографии для конфиденциальности и шифрованного сообщения аутентификационного кода для надежности сообщений.

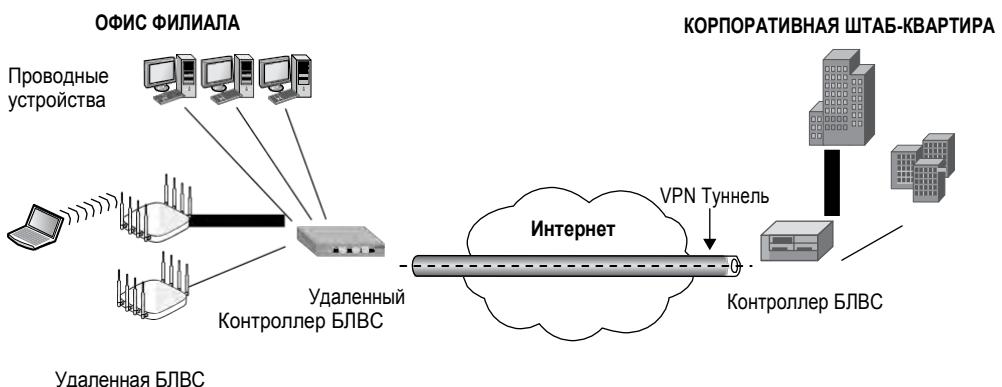
Хотя большинство решений IPsec VPN являются NAT-пересекающими [*NAT-transversal*], SSL VPNы часто выбираются из-за проблем с NATом или ограничительных политик межсетевого крана на удаленных местах.

## Развертывание VPN

VPNы наиболее часто используются для безопасности на основе клиента [*client-based security*], при подключении к БЛВСам публичного доступа и хотспотам, которые не обеспечивают безопасность. Так как большинство хотспотов не обеспечивают безопасность WI-Fi, крайне важно, чтобы конечные пользователи обеспечивали свою собственную безопасность. Технология VPN может предоставить необходимый уровень безопасности для удаленного доступа, когда конечные пользователи подключаются к БЛВСам публичного доступа. Поскольку никакого шифрования не используется в БЛВСах публичного доступа, то обычно нужно VPN решение для обеспечения конфиденциальности данных, как показано на Рисунке 17.18.

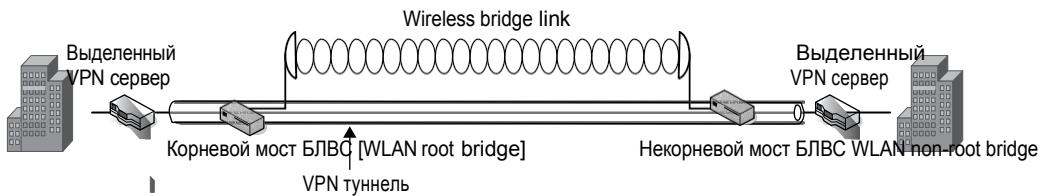
**РИСУНОК 17.18** VPN, установленный из публичного хотспота

Еще одно типовое использование технологии VPN - это предоставление соединения место-место или точка-точка [site-to-site] между удаленным офисом и корпоративным офисом. Большинство производителей БЛВС теперь предлагают клиент-серверный функционал и в своих ТД и в контроллерах БЛВС. Как показано на Рисунке 17.19, контроллер БЛВС офиса филиала с поддержкой VPN может туннелировать трафик клиента БЛВС и трафик проводной части и соединить с корпоративной сетью. Другие производители БЛВС также могут туннелировать пользовательский трафик с ТД для шлюза VPN сервера.

**РИСУНОК 17.19** VPN точка-точка [Site-to-site]

Еще одно использование VPNов – это обеспечение безопасности беспроводным мостам 802.11 [802.11 WLAN bridges links]. В дополнение к использованию для предоставления клиентского доступа, технология 802.11 используется для создания сетевых мостов между двумя или более локациями. Когда мосты БЛВС развернуты для беспроводной транзитной связи, технология VPN может быть использована для обеспечения необходимого уровня конфиденциальности данных. В зависимости от используемого оборудования для создания моста, поддержка VPN может быть интегрирована в мосты, или вам может понадобиться использовать другие устройства или программное обеспечение для поддержки VPN. Рисунок 17.20 показывает пример беспроводного сетевого моста точка-точка, использующего выделенные VPN устройства. VPN туннель точка-точка [site-to-site] используется для предоставления шифрования связи 802.11 между двумя мостами БЛВС.

РИСУНОК 17.20 Мост БЛВС и безопасность с VPN



## ИТОГО

В этой главе вы узнали, что пять главных компонентов нужны для беспроводной безопасности. Нужны решения надежного шифрования, чтобы защитить кадры данных. Нужно решение по безопасной аутентификации, чтобы гарантировать, что только законные пользователи авторизованы для использования сетевых ресурсов. Необходимо решение по сегментации, чтобы далее разграничить какие пользователи к каким ресурсам могут иметь доступ и куда они могутходить. Беспроводные сети 802.11 могут быть далее защищены непрерывным мониторингом и усиленным применением политики безопасности БЛВС. Мы обсуждали устаревшие решения аутентификации и шифрования 802.11, и почему они являются ненадежными. Мы охватили более сильные решения аутентификации 802.1X/EAP и преимущества динамической генерации ключей шифрования, а также что определено стандартом 802.11-2020 и соответствующей сертификацией WPA/WPA2. Стандарт 802.11-2020 определяет надежную защищенную сеть 2ого уровня, использующую аутентификацию или 802.1X/EAP, или PSK. Шифрование CCMP/AES предназначено Wi-Fi Альянсом для сертификации WPA2 и было преобладающим методом шифрования в БЛВС почти 15 лет. Сертификация Wi-Fi Альянса WPA3 определяет новые улучшения безопасности такие как аутентификация SAE. Принятие безопасности WPA3 только началось и будет обязательным в полосе частот 6 ГГц.

Безопасность Wi-Fi работает на уровне 2 модели OSI; однако, учет безопасности верхних уровней все еще необходим. Когда Wi-Fi клиенты аутентифицированы, часто используется сегментация трафика посредством VLANов и RBAC для управления безопасностью на более высоких уровнях.

Наконец, мы обсудили как технология VPN используется в средах БЛВС. Важно понимать, какие есть возможности и ограничения у устройств, которые будут развернуты в вашей беспроводной сети 802.11. Идеально, когда устройства будут сегментированы по разным VLANам и политикам доступа с помощью аутентификации 802.1X/EAP и шифрования CCMP/AES. VoIP телефоны, мобильные сканеры, планшеты, ручные устройства, и так далее часто не оснащены возможностью работать с более продвинутыми характеристиками безопасности. Надлежащие проекты по безопасности должны принимать во внимание все эти компоненты, чтобы гарантировать самую динамичную и безопасную сеть.

# Темы Экзамена

**Дать определение концепции AAA.** Суметь объяснить различия между аутентификацией, авторизацией, и учетом, и почему каждое необходимо для сетей БЛВС.

**Объяснить, почему нужна конфиденциальность данных.** Суметь обсудить почему кадры данных должны быть защищены шифрованием. Знать различия между различными шифрами шифрования.

**Понимать устаревшую безопасность 802.11.** Идентифицировать и понимать аутентификацию Открытой Системы [Open System] и аутентификацию с Общим Ключом [Shared Key]. Понимать, как работает шифрование WEP и знать ее слабости.

**Объяснить структуру 802.1X/EAP.** Быть способным объяснить все компоненты решения 802.1X и протокола аутентификации EAP. Понимать, что генерация динамических ключей шифрования является побочным продуктом взаимной аутентификации.

**Объяснить требования надежной безопасной сети.** Понимать, что стандарт 802.11-2020 конкретно определяет надежную безопасность [robust security] и уметь противопоставить что определено для WPA и WPA2 сертификаций.

**Понимать TKIP/ARC4, CCMP/AES и GCMP/AES.** Уметь объяснить основы каждого метода шифрования. Понимать 4x-Стороннее Рукопожатие и симбиоз между аутентификацией и генерацией динамических ключей шифрования.

**Объяснить разницу между безопасностью WPA, WPA2, WPA3, и Улучшенной Открытостью [Enhanced Open].** Объяснить аутентификацию и требования к шифрованию для каждой версии сертификации безопасности Wi-Fi Альянса.

**Объяснить зачем нужна сегментация.** Понимать, как VLANы и политики доступа на основе ролей используются для дальнейшего ограничения к сетевым ресурсам.

**Объяснить безопасность VPN БЛВС [VPN WLAN security].** Определить основы технологии VPN и когда он может быть использован в среде БЛВС.

# Контрольные вопросы

1. Какие механизмы БЛВС требуют, чтобы каждый пользователь БЛВС имел уникальные учетные данные аутентификации? (Выберите все, что применимо.)

  - A. Открытая Система [Open System]
  - B. WPA-Personal
  - C. WPA2-Personal
  - D. WPA2-Enterprise
  - E. WPA3-Personal
  - F. WPA3-Enterprise
2. В соответствии с тем, как определено Wi-Fi Альянсом в сертификации безопасности, какой режим работы требует использование 256-битного Протокола Режима Счетчика/Галуа [256-bit Galois/Counter Mode Protocol (GCMP-256)] для шифрования данных?

  - A. WPA3-Personal only
  - B. WPA3-Personal transition
  - C. WPA3-Enterprise only
  - D. WPA3-Enterprise transition
  - E. WPA3-Enterprise 192-bit
3. 128-битное WEP шифрование использует предоставляемый пользователем статический ключ какого размера?

  - A. 104 байта
  - B. 64 бита
  - C. 124 бит
  - D. 128 бит
  - E. 104 бита
4. Какие три главных компонента составляют структуру авторизации 802.1X?

  - A. Клиент [Supplicant]
  - B. База данных LDAP [LDAP database]
  - C. Сервер Аутентификации [Authentication server]
  - D. Расчетный излучатель [Intentional radiator]
  - E. Аутентификатор [Authenticator]
5. Какой из этих методов безопасности является заменой аутентификации PSK, в соответствии с определением WPA3?

  - A. PSK для каждого пользователя/для каждого устройства [Per-user/per-device PSK ]
  - B. Установка Защищенного Wi-Fi [Wi-Fi Protected Setup (WPS)]

- C. Одновременная аутентификация равных [Simultaneous authentication of equals (SAE)]
  - D. EAP-SIM
  - E. WPA2-Personal
6. Компания АКМЕ использует WPA2-Personal для защиты IoT устройств, которые не поддерживают аутентификацию of 802.1X/EAP . Так как сотрудник недавно был уволен, то все беспроводные устройства IoT компании и ТД нужно перенастроить на новый статический 64-битный PSK. Какой тип решения безопасности БЛВС может устраниить эту административную головную боль?
- A. MAC фильтр [MAC filter]
  - B. Скрытый SSID [Hidden SSID]
  - C. Изменение заводских настроек
  - D. PSK на каждое устройство, на каждого пользователя [Per-device, per-user PSK]
7. Какой из следующих методов шифрования использует симметричные шифры? (Выберите все, что применимо.)
- A. WEP
  - B. TKIP
  - C. Криптография с открытым-ключом [Public-key cryptography]
  - D. CCMP
8. Что утверждает стандарт IEEE 802.11-2020 из следующего относительно скорости передачи данных 802.11n, 802.11ac, и 802.11ax и шифрования? (Выберите все, что применимо.)
- A. WEP и TKIP должны не использоваться.
  - B. CCMP и GCMP могут использоваться.
  - C. WEP не может использоваться; однако, TKIP может использоваться, если также используется 802.1X.
  - D. Любой метод шифрования, определенный стандартом, может использоваться.
9. Когда развернута безопасность 802.1X/EAP, RADIUS атрибуты также могут использоваться для назначений на основе ролей какого типа разрешений пользовательского доступа? (Выберите все, что применимо.)
- A. Правила межсетевого экрана с контролем состояния [Stateful firewall rules]
  - B. Время [Time]
  - C. VLANs
  - D. ACLs
  - E. Полоса [Bandwidth]
10. Как используется IPsec VPNs для обеспечения безопасности в комбинации с 802.11 WLANs?
- A. Безопасность на основе клиента в БЛВС с публичным доступом
  - B. Каналы связи – беспроводной мост точка-точка
  - C. Связь через WAN каналы связи
  - D. Все выше перечисленное.

- 11.** Когда включено, шифрование БЛВС обеспечивает конфиденциальность данных для какой части кадра данных 802.11?
- A.** MPDU
  - B.** MSDU
  - C.** PPDU
  - D.** PSDU
- 12.** Какой из следующих методов аутентификации должен происходить вместе с 4x-Сторонним Рукопожатием для того, чтобы сгенерировать динамические ключи шифрования CCMP/AES? (Выберите все, что применимо.)
- A.** Аутентификация с Общим Ключом и 4x-Стороннее Рукопожатие [Shared Key authentication and 4-Way Handshake]
  - B.** Аутентификация 802.1X/EAP и 4-х Стороннее Рукопожатие [802.1X/EAP authentication and 4-Way Handshake]
  - C.** Статический WEP и 4x-Стороннее Рукопожатие [Static WEP and 4-Way Handshake]
  - D.** Аутентификация PSK и 4x-Стороннее Рукопожатие [PSK authentication and 4-Way Handshake]
  - E.** Аутентификация SAE и 4x-Стороннее Рукопожатие [SAE authentication and 4-Way Handshake]
- 13.** Для того, чтобы решение 802.1X/EAP работало надлежащим образом, какие два компонента должны оба поддерживать один и тот же тип EAP?
- A.** Клиент [Supplicant]
  - B.** Авторизатор [Authorizer]
  - C.** Аутентификатор [Authenticator]
  - D.** Сервер Аутентификации [Authentication server]
- 14.** Когда вы используете решение с беспроводным контроллером 802.11, какое устройство обычно работает как аутентификатор?
- A.** Точка доступа
  - B.** LDAP сервер
  - C.** Контроллер БЛВС
  - D.** RADIUS сервер
- 15.** Какой из этих вариантов использования применения аутентификации PSK на каждого пользователя/на каждое устройство [per-user/per-device] не рекомендуется?
- A.** Уникальные учетные данные для устройств BYOD
  - B.** Уникальные учетные данные для устройств IoT
  - C.** Уникальные учетные данные для гостевого Wi-Fi доступа
  - D.** Уникальные учетные данные для устаревших корпоративных устройств без поддержки 802.1X/EAP
  - E.** Уникальные учетные данные для корпоративных устройств с поддержкой 802.1X/EAP
- 16.** Что успешно обеспечивает 802.1X/EAP, когда надлежащим образом применен для безопасности БЛВС? (Выберите все, что применимо.)
- A.** Доступ к сетевым ресурсам
  - B.** Подтверждение учетных данных точки доступа

- C. Динамическую аутентификацию
  - D. Динамическое создание ключей шифрования
  - E. Подтверждение пользовательских учетных данных
- 17. CCMP шифрование использует какой размер AES ключа?
  - A. 192 бит
  - B. 64 бита
  - C. 256 бит
  - D. 128 бит
- 18. Идентифицируйте решение безопасности, которое определено Сертификацией WPA2 Wi-Fi Альянса (Выберите все, что применимо.)
  - A. Аутентификация 802.1X/EAP
  - B. Динамические шифрование WEP
  - C. Аутентификация SAE
  - D. Аутентификация PSK
  - E. Шифрование DES
  - F. Шифрование CCMP
- 19. Какие требования опционального 192-битного режима WPA3-Enterprise определены Wi-Fi Альянсом? (Выберите все, что применимо)
  - A. CCMP/AES with 128-bit encryption of data frames
  - B. BIP-GMAC-256 for management frame protection
  - C. EAP-TLS authentication protocol
  - D. EAP-TTLS authentication protocol
  - E. 256-bit GCMP/AES encryption of data frames
  - F. BIP-CMAC-128 for management frame protection
- 20. Какой протокол 2ого уровня используется для аутентификации в структуре 802.1X?
  - A. RSN
  - B. SAE
  - C. EAP
  - D. PAP
  - E. CHAP

# Глава 18



## Приноси Свое Собственное Устройство (BYOD) и Гостевой Доступ

**В ЭТОЙ ГЛАВЕ ВЫ УЗНАЕТЕ О СЛЕДУЮЩЕМ:**

✓ **Управление мобильными устройствами (MDM)**

- Устройства компании или персональные устройства
- Архитектура MDM
- Регистрация в системе MDM
- Профили MDM
- Программный агент MDM
- Управление через эфир [Over-the-air management]
- Управление приложениями

✓ **Самостоятельная регистрация устройств сотрудников**

- Регистрация с двумя SSID
- Регистрация с одним SSID
- MDM или Самостоятельная Регистрация

✓ **Доступ в гостевую БЛВС**

- Гостевой SSID
- Гостевой VLAN
- Гостевая политика межсетевого экрана
- Перехватывающие веб порталы
- Изоляция клиентов, ограничение скорости, и фильтр содержимого веб.
- Управление Гостевым доступом
- Самостоятельная регистрация гостей



- Поручительство Сотрудников

- Логин Социальной Сети

- Шифрованный гостевой доступ

✓ **Хотспот 2.0 и Пасспоинт**

- Протокол Опроса Сетей Доступа

- Архитектура Хотспот 2.0

- 802.1X/EAP и Хотспот 2.0

- Онлайн регистрация

- Роуминговые соглашения

✓ **Контроль сетевого доступа (NAC)**

- Состояние

- Отпечаток ОС

- AAA

- Изменение Авторизации (CoA) по RADIUS

- Единый вход [Single Sign-On]

- SAML

- OAuth



Многие годы основной целью корпоративных БЛВС было предоставление беспроводного доступа для ноутбуков, принадлежащих компаниям, используемых сотрудниками.

Некоторые вертикальные рынки, такие как медицина, розница, и производство, также требуют доступ к БЛВС для мобильных устройств, принадлежащих компаниям, такие как VoWiFi телефоны и беспроводные сканеры штрих-кодов. Более 13 последних лет, однако, был бурный рост парка мобильных персональных устройств с Wi-Fi. Wi-Fi радиомодули теперь являются основными компонентами связи в смартфонах, планшетах, ПК и многих других мобильных устройствах.

Хотя мобильные устройства изначально были предназначены для персонального использования, организации нашли способы применения корпоративных мобильных устройств с доработанным программным обеспечением для улучшения продуктивности и функциональности. Сотрудники также все больше хотели использовать свои персональные мобильные устройства на рабочем месте. Сотрудники ожидают, что они смогут подключиться к корпоративной БЛВС несколькими персональными мобильными устройствами. Популярное выражение *приноси свое собственное устройство* [*bring your own device (BYOD)*] относится к политике разрешения сотрудникам приносить собственные мобильные устройства, такие как смартфоны, планшеты, и ноутбуки на свои рабочие места. Политика BYOD описывает, какие корпоративные ресурсы могут или не могут быть доступны, когда сотрудники подключаются к БЛВС компании своими персональными устройствами. Политика BYOD обычно также определяет, как устройствам сотрудников разрешено подключаться к БЛВС.

Главный фокус этой главы в объяснении того как используется безопасность для контроля и мониторинга BYOD доступа к БЛВС. Решения управления мобильными устройствами [*Mobile device management (MDM)*] могут быть использованы для удаленного управления и контроля мобильных Wi-Fi устройств компании и персональных устройств. Решения MDM используют программный сервер или облачные сервисы для конфигурирования клиентских настроек, вместе с клиентскими приложениями, и для контроля и мониторинга того, что могут делать пользователи. Дополнительно, есть растущая тенденция по использованию решений с самостоятельной регистрацией BYOD, где сотрудники могут безопасно предоставить свои личные устройства БЛВС. Контроль сетевого доступа [*Network access control (NAC)*] интегрирует разные технологии, такие как AAA, RADIUS, проверки состояния клиента, гостевые сервисы, и самостоятельная регистрация клиента и просто регистрация. С помощью этих технологий NAC может контролировать и мониторить клиентский доступ на сети. NAC может быть использован для обеспечения аутентификации и контроля доступа управляемых MDM устройств, корпоративных Wi-Fi устройств, или устройства сотрудников (BYOD) и гостевые устройства.

Эта глава также охватывает многие компоненты БЛВС гостевого доступа, и как он с годами развивался. Технология гостевого доступа включает поддержку устройств посетителей вместе с BYOD устройствами сотрудников.

# Управление Мобильными Устройствами

*Консьюмеризация IT* [*Consumerization of IT*] - это фраза, используемая для описания сдвига в информационных технологиях, которые начинаются на потребительском рынке идвигаются на предприятия и правительственные учреждения. Становится общепринятым для сотрудников приносить устройства потребительского рынка на рабочее место, после того, как эта новая технология уже опробована дома. В ранние дни Wi-Fi большинство предприятий не предоставляло беспроводной сетевой доступ к корпоративной сети. Из-за ограниченных вариантов беспроводной безопасности, доступных в то время, вместе с общим недоверием к неизвестному, было обычным для компаний избегать внедрения БЛВС. Однако, так как пользователям нравилась гибкость Wi-Fi дома, они начали приносить беспроводные маршрутизаторы для небольших и домашних офисов [small office/home office (SOHO)] в офис и устанавливать их, несмотря на возражение IT департамента. В конечном счете, предприятия и государственные организации осознали, что им необходимо устанавливать БЛВС, чтобы воспользоваться их преимуществами, а также управлять технологией.

Персональные мобильные Wi-Fi устройства, такие как смартфоны и планшеты, существуют уже довольно много лет. Apple iPhone был впервые представлен в Июне 2007 года, а первый iPad дебютировал в Апреле 2010 года. НТС [эйч-ти-си] представила первый смартфон на Android в Октябре 2008 года. Эти устройства изначально предназначались для персонального использования, но за короткое время, сотрудники захотели также использовать свои персональные устройства в БЛВС компаний. Дополнительно, разработчики программного обеспечения начали создавать корпоративные мобильные бизнес приложения для смартфонов и планшетов. Предприятия начали покупать и устанавливать планшеты и смартфоны, чтобы использовать преимущества этих мобильных корпоративных приложений. Планшеты и смартфоны предоставляли реальную мобильность, которую желали сотрудники и компании. В течении нескольких лет количество мобильных устройств, подключающихся к корпоративным БЛВС превысило число подключений ноутбуков. Эта тенденция сохраняется со многими, если не со всеми устройствами, поставляемыми с WI-FI в качестве основного сетевого адаптера. Многие ноутбуки теперь поставляются без Ethernet адаптера, потому что Wi-Fi радиомодуль ноутбука используется для доступа к сети.

Из-за быстрого распространения персональных мобильных устройств, понадобилась политика BYOD, чтобы определить, как персональные устройства сотрудников могут получать доступ к корпоративной БЛВС. Решение по управлению мобильными устройствами [mobile device management (MDM)] для принятия персональных мобильных устройств, а также устройств компаний в БЛВС. Корпоративные IT отделы могут развернуть MDM сервера для управления, защиты, и мониторинга мобильных устройств. Решения MDM могут управлять устройствами с разными мобильными операционными системами и разными мобильными сервис провайдерами. Большинство решений MDM используются для управления мобильными устройствами на iOS и Android. Однако, мобильные устройства, которые используют другие операционные системы, такие как BlackBerry OS, также могут управляться решениями MDM.

Хотя главный фокус решения MDM это управление смартфонами и планшетами, некоторые решения MDM также могут быть использованы для принятия в сеть персональных ноутбуков с macOS и Chrome OS. Несколько беспроводных устройств, которые могут управляться решением MDM показаны на Рисунке 18.1.

Некоторые производители инфраструктуры БЛВС разработали мелко-масштабные решения MDM, специально предназначенные для их решений по управлению сетью [NMS]. Однако, большие компании MDM продают устанавливаемые поверх решения, которые могут быть использованы с решениями любых производителей БЛВС.

**РИСУНОК 18.1** Персональные мобильные устройства с Wi-Fi радиомодулями

Вот некоторые из основных производителей, продающих устанавливаемые поверх решения MDM:

VMware AirWatch—[www.air-watch.com](http://www.air-watch.com)

Citrix—[www.citrix.com](http://www.citrix.com)

IBM—[www.maas360.com](http://www.maas360.com)

Jamf Software—[www.jamfsoftware.com](http://www.jamfsoftware.com)

MobileIron—[www.mobileiron.com](http://www.mobileiron.com)

Вы можете пересечься с другой терминологией, при работе с MDM. Например, некоторые производители используют термин *управление корпоративной мобильностью* [*enterprise mobility management (EMM)*]. Дополнительно, MDM начал эволюционировать в *унифицированное управление оконечным оборудованием* [*unified endpoint management (UEM)*]. Решение UEM предоставляет корпоративное управление мобильными устройствами, а также проводными устройствами, такими как принтеры, настольные устройства, носимые устройства, и IoT устройствами из одной платформы управления.

## Устройства Компании или Персональные Устройства

Решение MDM может быть использовано для управления и устройствами компании и персональными устройствами. Однако, управление устройствами компании и персональными устройствами совершенно различно. Мобильное устройство компании было приобретено компанией с целью повышения производительности сотрудника. Планшет или смартфон мог быть выдан индивидуальному сотруднику или быть общим для сотрудников разных смен. На этих устройствах установлены коммерческие бизнес приложения, а часто отраслевые приложения. Многие компании даже разрабатывают собственные приложения, уникальные для их собственных бизнес нужд. Мобильные устройства компании

**846** Глава 18 • Приноси Свое Собственное Устройство (BYOD) и Гостевой Доступ часто развертываются для замены старого оборудования. Например, программа по контролю имущества, работающая на планшете, может заменить устаревший ручной сканер штрих-кодов. Программное приложение Голос поверх Интернет Протокола [Voice over Internet Protocol] (VoIP), работающее на смартфоне, может быть использовано для замены старых трубок VoWiFi. IT департамент обычно будет выбирать одну модель мобильных устройств, которые работают на одной и той же операционной системе.

Стратегия управления для мобильных устройств компании обычно определяет более глубокую безопасность, потому что часто на устройствах компании хранятся корпоративные документы и информация. Когда устройства компании управляются решением MDM, то включены многие конфигурационные настройки, такие как клиентский доступ через виртуальную частную сеть [VPN], настройка учетной записи электронной почты, настройки Wi-Fi профиля, настройки паролей и шифрования. Возможность удаления MDM профиля с устройства компании сотрудником отключена, и администратор MDM может удаленно очистить мобильные устройства компании, если они потерялись или украдены. Решение MDM также используется для инвентарного контроля оборудования и программного обеспечения. Так как эти устройства не являются персональными устройствами, IT департамент также может указать какие приложения могут или не могут быть установлены на планшеты и/или смартфоны.

Концепция BYOD появилась, потому что персональные мобильные устройства сложно контролировать и управлять ими при предоставлении доступа к корпоративной сети. Доступ и контроль может контролироваться с помощью MDM или решения контроля сетевого доступа (NAC), но потребности BYOD отличаются от корпоративных потребностей. Сотрудники, посетители, поставщики, подрядчики, и консультанты приносят широкий спектр персональных устройств — различные марки и модели, загруженные различными операционными системами и приложениями—на рабочее место. Следовательно, нужна другая стратегии управления для BYOD. У каждой компании должна быть своя собственная уникальная стратегия сдерживания BYOD, при этом разрешающая доступ к корпоративной БЛВС. Например, когда персональные устройства управляются решением MDM, то камера может быть отключена так, чтобы нельзя было сделать фотографию внутри здания. Как показано на Рисунке 18.2, множество ограничений может быть принудительно применено на устройствах компании или персональных устройствах после включения их в решение MDM.

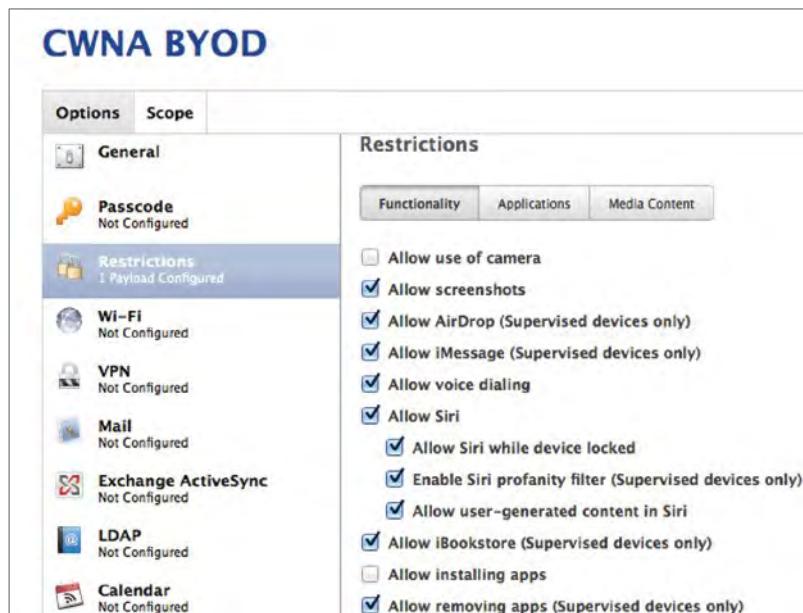
Как альтернатива решению MDM может использоваться решение NAC для аутентификации персональных устройств вместе с контролем доступа к сетевым ресурсам без необходимости установки программного обеспечения на клиентское устройство. Решение NAC не предоставляет контроль над индивидуальным устройством, но может обеспечить исчерпывающий контроль над уровнем доступа персонального устройства на сети. Решения NAC могут предписывать минимальные требования по безопасности, например, антивирусную защиту, прежде чем устройству будет разрешено иметь доступ к сети. Более детальное обсуждение о NAC можно найти позже в этой главе.

## Архитектура MDM

Базовая архитектура любого решения MDM состоит из следующих четырех главных компонентов:

**Мобильное Устройство** Мобильному Wi-Fi устройству требуется доступ к корпоративной БЛВС. Мобильное устройство может быть или устройством компании, или устройством сотрудника. В зависимости от производителя MDM, могут поддерживаться несколько операционных систем, включая iOS, Android, Chrome OS, и macOS, среди прочих. Мобильные устройства не допускаются в корпоративную сеть, до тех пор, пока процесс регистрации устройства не завершен, и не установлен MDM профиль.

РИСУНОК 18.2 Ограничения устройства [Device restrictions]



**ТД/Контроллер БЛВС** Вся Wi-Fi связь осуществляется между мобильными устройствами и точкой доступа, к которой они подключены. Если устройства не заведены в сервере MDM, ТД или контроллер БЛВС помещает мобильные устройства в карантин внутрь ограниченной области сети, называемой *огороженный сад* [*walled garden*]. Мобильным устройствам, которые включены через процесс регистрации, разрешен доступ за пределы огороженного сада [*walled garden*].

**MDM Сервер** MDM сервер отвечает за регистрацию клиентских устройств. MDM сервер обеспечивает мобильные устройства MDM профилями, которые определяют ограничения клиентских устройств, а также конфигурационные настройки. MDM сервер может обеспечивать сертификатами. MDM серверы также могут быть настроены на белые и черные списки. Политики белых списков [*whitelisting*] ограничивают регистрацию списком определенных устройств и операционных систем. Политики черных списков [*blacklisting*] позволяют регистрироваться всем устройствам и операционным системам, кроме тех, конкретных, запрещенных черным списком. Хотя начальная роль MDM сервера заключается в обеспечении и принятии мобильных устройств в БЛВС, сервер также используется для мониторинга клиентских устройств. Контроль и настройка учтенных устройств [*device inventory*] являются ключевыми компонентами решения MDM. Сервер MDM обычно доступен как облачный сервис или как серверное решение, которое установлено в дата-центре компании. Локальные MDM серверы могут быть в форме аппаратного комплекса или в виде программного обеспечения в виртуальной серверной среде.

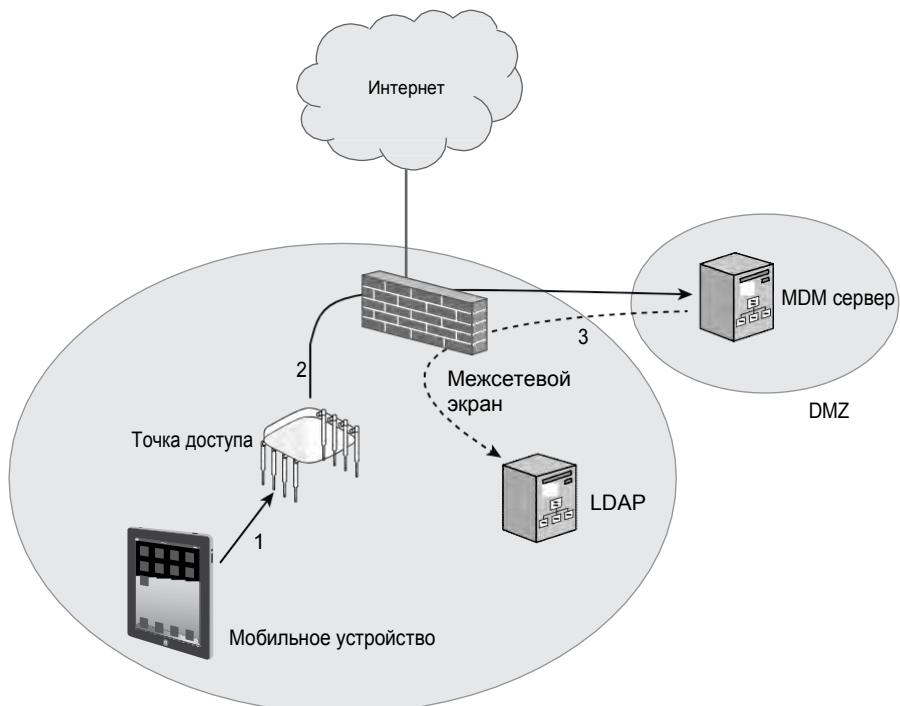
**Серверы Push Уведомлений** MDM сервер взаимодействует с серверами push уведомлений, такими как *сервис Push Уведомлений Apple* [*Apple Push Notification service (APNs)*] и *Облачные Сообщения Google* [*Google Cloud Messaging (GCM)*], для управления через эфир [*over-the-air management*] мобильными Wi-Fi устройствами. Управление через эфир обсуждается более детально позже в этой главе.

Установка MDM архитектуры включает другие ключевые компоненты. MDM серверы могут быть настроены на связь с базами данных *Облегченного Протокола Доступа к Каталогу* [*Lightweight Directory Access Protocol (LDAP)*], таких как Активный Каталог [Active Directory]. Обычно также размещаются корпоративные межсетевые экраны. Соответствующие исходящие порты должны быть открыты, чтобы разрешить связь между всеми различными компонентами архитектуры MDM. Например, порт 443 Протокола Контроля Передачи [Transmission Control Protocol (TCP)] должен быть открыт для шифрованной SSL связи между ТД и MDM сервером, а также SSL связь между мобильным устройством и MDM сервером. TCP порт 5223 должен быть открыт, чтобы мобильные устройства могли взаимодействовать с APNs. TCP порты 2195 и 2196 нужны для трафика между MDM сервером и APNs. TCP порты 443, 5223, 5229, и 5330 требуются для связи между мобильными устройствами и GCM. Связь между MDM сервером и GCM требует, чтобы был открыт TCP порт 443.

## Регистрация в системе MDM

Когда установлена архитектура MDM, мобильные устройства должны пройти через процесс регистрации [enrollment process] для того, чтобы получить доступ к сетевым ресурсам. Процесс регистрации может быть использован для принятия в сеть и устройств компании и персональных устройств. Рисунок 18.3 иллюстрирует три первых шага процесса регистрации в системе MDM.

**РИСУНОК 18.3** Регистрация в системе MDM—начальные шаги



**Шаг 1: Мобильное устройство подключается к точке доступа.** Мобильное устройство должно сначала установить ассоциацию с ТД. Безопасность Wi-Fi может быть открытой, но обычно устройства компании или персональные устройства пытаются установить соединение с безопасным корпоративным SSID, который использует 802.1X/EAP или безопасностью с заранее известным общим ключом (PSK). В этой точке, ТД держит мобильное клиентское устройство внутри *огороженного сада* [walled garden]. Внутри развернутой сети *огороженный сад* [walled garden] - это закрытая среда, которая ограничивает доступ к содержимому веб и сетевым ресурсам, в то же время разрешая доступ к некоторым ресурсам. Огороженный сад [walled garden] является закрытой платформой сетевых сервисов, предоставленной для устройств и/или пользователей. Находясь внутри огороженного сада [walled garden] определенной ТД, единственные сервисы, которые доступны мобильным устройствам: Протокол Динамической Настройки Хоста [Dynamic Host Configuration Protocol (DHCP)], Система Доменных Имен [Domain Name System (DNS)], сервисы push уведомлений, и сервер MDM. Чтобы выйти из огороженного сада [walled garden], мобильное устройство должно найти соответствующую точку выхода, как в реальном огороженном саду. Назначенная точка выхода для мобильных устройств – это процесс регистрации в системе MDM.

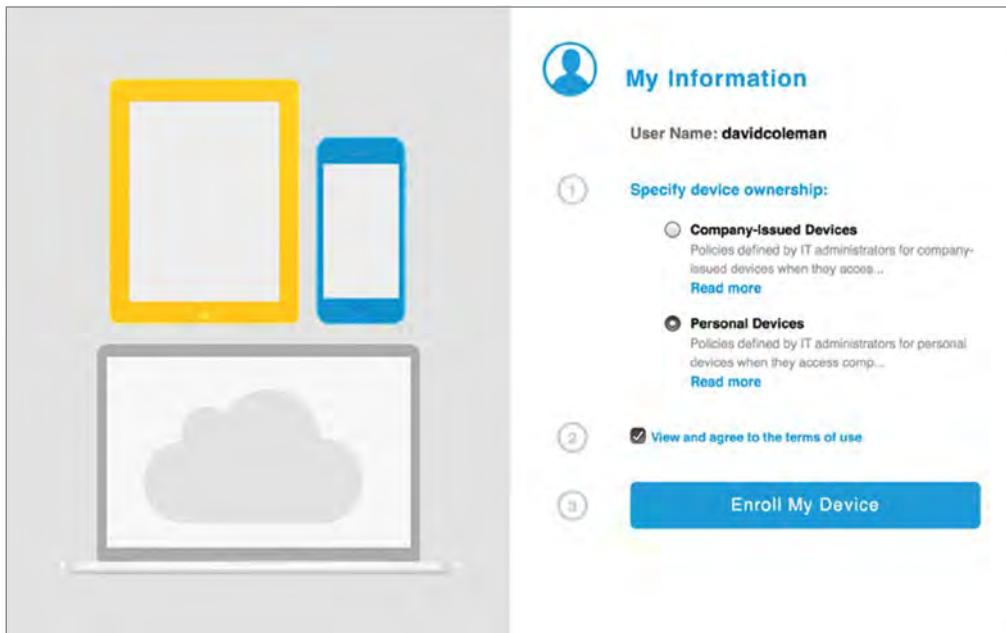
**Шаг 2: ТД проверяет зарегистрировано ли устройство.** Следующий шаг - определение зарегистрировано ли мобильное устройство. В зависимости от производителя БЛВС, ТД или контроллер БЛВС запрашивает MDM сервер, чтобы определить статус регистрации мобильного устройства. Если MDM предоставляется как облачный сервис, опрос по поводу регистрации проходит через WAN канал связи. Собственные MDM серверы обычно устанавливаются в демилитаризованной зоне (DMZ). Если мобильное устройство уже зарегистрировано, MDM сервер отправит сообщение ТД, чтобы выпустили устройство из огороженного сада [walled garden]. Незарегистрированные устройства будут оставаться на карантине внутри огороженного сада [walled garden].

**Шаг 3: MDM сервер спрашивает LDAP.** Хотя процесс регистрации может быть открытым, администраторы часто требуют аутентификацию. MDM сервер спрашивает существующую базу данных LDAP, например Активный Каталог [Active Directory]. LDAP сервер отвечает на вопрос, и затем регистрация в системе MDM может быть продолжена.

**Шаг 4: Устройство перенаправляется на MDM сервер.** Хотя незарегистрированное устройство имеет доступ к DNS сервисам, у устройства в карантине нет доступа к веб сервисам, кроме MDM сервера. Когда пользователь открывает браузер на мобильном устройстве, он перенаправляется на перехватывающий веб портал [captive web portal] для MDM сервера, как показано на Рисунке 18.4. Процесс регистрации может быть продолжен. По юридическим и конфиденциальным причинам перехватывающие веб порталы [captive web portals] содержат соглашение об отказе от юридической ответственности [legal disclaimer agreement], которое дает администратору MDM возможность ограничить настройки и удаленно изменить возможности мобильного устройства. Юридический отказ от ответственности особенно важен в ситуации BYOD, где сотрудники включают в сеть свои собственные персональные устройства. Если пользователи не соглашаются с юридическим отказом от ответственности, они не могут продолжить процесс регистрации и не будут выпущены из огороженного сада [walled garden].

**Шаг 5: Устройство устанавливает сертификаты и MDM профиль.** Если регистрация началась, то нужен процесс безопасного обеспечения через эфир [*over-the-air provisioning*] мобильного устройства всем необходимым для установки MDM профиля. Обеспечение через эфир [*over-the-air provisioning*] различается между операционными системами, но использование доверенных сертификатов и SSL шифрования является обычным. Например, мы опишем как происходит обеспечение [*provisioning*] устройств iOS. Для iOS устройств *Протокол Простой Установки Сертификатов* [*Simple Certificate Enrollment Protocol (SCEP)*] использует сертификаты и шифрование Уровня Безопасных Сокетов, чтобы защитить профили MDM. Пользователь мобильного устройства принимает начальный профиль, который установлен на устройстве.

РИСУНОК 18.4 MDM сервер—перехватывающий веб портал—шаг 4



После установки начального профиля, конкретная идентификационная информация устройства посыпается на MDM сервер. MDM сервер, затем посыпает полезную нагрузку SCEP, которая инструктирует мобильное устройство как загрузить доверенный сертификат из Центра Сертификации MDM [MDM certificate authority (CA)] или стороннего Центра Сертификации (CA). Когда сертификат установлен на мобильное устройство, полезная нагрузка из зашифрованного профиля MDM и настройкой ограничений безопасно отправляется на мобильное устройство и устанавливается там. Рисунок 18.5 изображает установку MDM профиля с помощью SCEP на устройство iOS.

**Шаг 6: Сервер MDM выпускает мобильные устройства.** Как показано на Рисунке 18.6, если устройство завершило MDM регистрацию, MDM сервер отправляет сообщение ТД или контроллеру БЛВС, чтобы выпустили мобильной устройство из огороженного сада [walled garden].

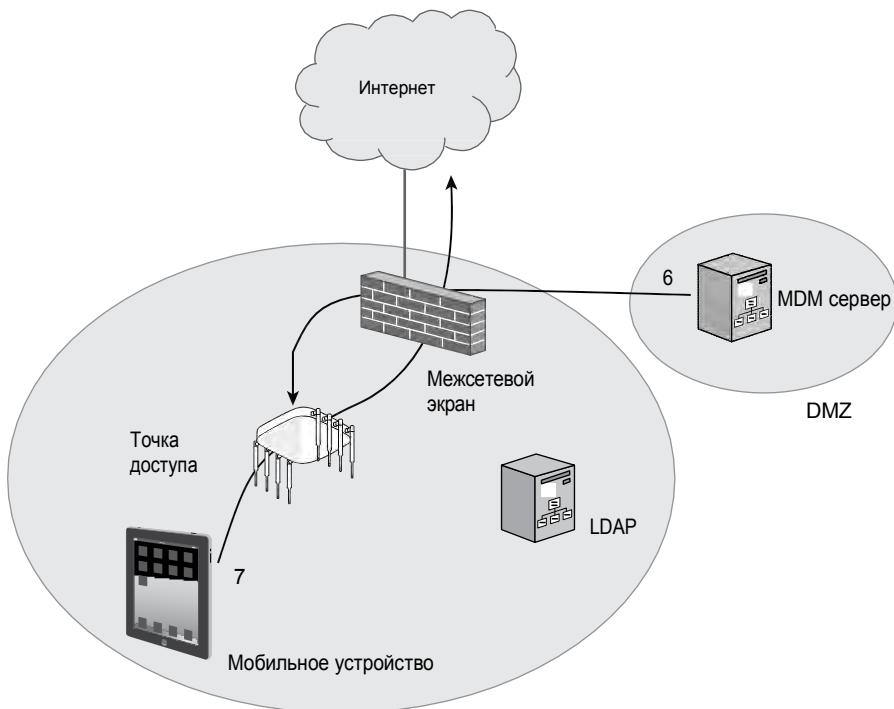
**Шаг 7: Мобильное устройство выходит из огороженного сада [walled garden].**

Мобильное устройство теперь следует настройкам ограничений и конфигураций, определенных профилем MDM. Например, использование камеры мобильного устройства может быть больше не разрешено. Также могут быть предоставлены конфигурационные настройки, такие как электронная почта или настройки VPN. Теперь мобильное устройство может свободно выйти из огороженного сада [walled garden] и получить доступ в Интернет или к корпоративным сетевым ресурсам, как проиллюстрировано на Рисунке 18.6. Доступ к доступным сетевым ресурсам определяется типом устройства или идентификатором [identity] пользователя. Например, устройства компаний могут иметь доступ ко всем сетевым серверам, в то время как персональные устройства могут иметь доступ только к определенным серверам, таким как сервер электронной почты. Когда устройство выпущено из огороженного сада [walled garden], персональное устройство может быть помещено в VLAN только с доступом в Интернет, в то время как устройства компаний могут быть помещены в менее ограниченный VLAN.

**РИСУНОК 18.5** Установка Сертификата и MDM профиля—шаг 5



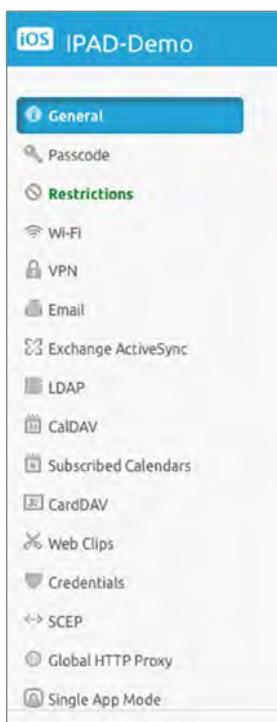
**РИСУНОК 18.6** Мобильное устройство выпущено из огороженного сада [walled garden]



## Профили MDM

Вы уже узнали, что MDM профили используются для ограничения мобильных устройств. Профили MDM также могут использоваться для глобальной настройки различных компонентов мобильных устройств. MDM профили - это фактически, конфигурационные настройки мобильных устройств. Как показано на примере на рисунке 18.7, MDM профили могут включать ограничения устройства, настройки электронной почты, настройки VPN, настройки службы каталога LDAP, и настройки Wi-Fi. MDM профили могут также включать вебзакладки [webclips], которые являются ссылками для браузера, которые указывают на определенные URLs. Иконка вебзакладки [webclip] автоматически устанавливается на экран мобильного устройства. Например, устройства компании могут быть оснащены вебзакладкой - ссылкой на внутренний интранет компании.

**РИСУНОК 18.7** Настройки MDM профиля



Конфигурационные профили, используемые устройствами с macOS и iOS - это файлы *Расширяемого Языка Разметки* [*Extensible Markup Lan- guage (XML)*]. У Apple есть несколько инструментов по созданию профилей, включающие Apple Configurator [Apple Конфигуратор] и iPhone Configuration Utility [Утилита Настройки iPhone]. Для ручной установки XML профили могут быть доставлены через электронную почту или через вебсайт. Ручная установка и настройка подходит для одного устройства, но как насчет всей компании, где тысячи устройств могут нуждаться в настройке? На предприятии, где нужен метод по автоматизации доставки конфигурационных или настроек профилей, приходит на помощь решение MDM. Конфигурационные профили MDM создаются на сервере MDM и устанавливаются на мобильных устройствах во время процесса регистрации.

Как упоминалось, один аспект MDM профиля в том, что могут быть автоматически предоставлены настройки Wi-Fi. Устройства компании могут быть жестко привязаны к определенному Wi-Fi профилю, в котором указан корпоративный SSID и соответствующие настройки безопасности. Профиль MDM также может быть использован для установки настроек Wi-Fi на персональные устройства сотрудников. Если развернуто 802.1X/EAP, то корневой сертификат ЦС [root CA certificate] должен быть установлен на клиентском мобильном устройстве. Решение MDM - это эффективный способ безопасной установки корневых сертификатов ЦС [root CA certificates] на мобильные устройства. Клиентские сертификаты также могут быть установлены, если выбран EAP-TLS для протокола безопасности 802.1X. Некоторые компании используют решение MDM только ради размещения сертификатов на клиентских устройствах БЛВС, из-за широкого разнообразия операционных систем.

MDM профили могут быть удалены с устройства локально или могут быть удалены удаленно через Интернет через сервер MDM.

### Могут Сотрудники Удалить MDM Профили с Мобильного Устройства?

Если мобильное устройство прошло через процесс регистрации, то на мобильном устройстве установлены конфигурационные профили MDM и соответствующие сертификаты. Следующая картинка показывает экран настроек iPad с установленными MDM профилиями.



Может ли сотрудник удалить профили MDM? Ответ на этот вопрос - это дело политики компании. Мобильные устройства компании обычно имеют жестко привязанные MDM профили и они не могут быть удалены. Это удерживает сотрудников от проведения неавторизованных изменений с устройством. Если мобильное устройство украдено, и на устройстве находится чувствительная информация, то администратор MDM может удаленно очистить мобильное устройство, если оно подключено к Интернет. Политика BYOD персональных устройств обычно менее жесткая. Когда сотрудник регистрирует

свое персональное устройство через корпоративное решение MDM, обычно сотрудник сохраняет возможность удалить профили MDM, потому что это его собственное устройство. Если сотрудник удаляет профили MDM, устройство больше не управляется корпоративным решением MDM. В следующий раз, когда сотрудник попытается подключиться к БЛВС компании с мобильного устройства, сотрудник должен будет снова проходить процесс регистрации в MDM системе.

## Программный Агент MDM

Операционные системы некоторых мобильных устройств требуют программное приложение - MDM агент [MDM agent]. Например, устройства на Android требуют приложение MDM агента подобного тому, которое показано на Рисунке 18.8. ОС Android является операционной системой с открытым исходным кодом, которая может быть адаптирована под различных производителей мобильных устройств. Хотя это предоставляет намного лучшую гибкость, управляемость и администрирование, устройства на Android на предприятии могут быть проблемой из-за огромного количества производителей оборудования. Приложение MDM-агент может сообщить уникальную информацию об устройстве на Android MDM серверу, которая позже может быть использована для MDM ограничений и конфигурационных политик. Агент MDM должен поддерживать нескольких производителей Android устройств.

РИСУНОК 18.8 Приложение MDM агент



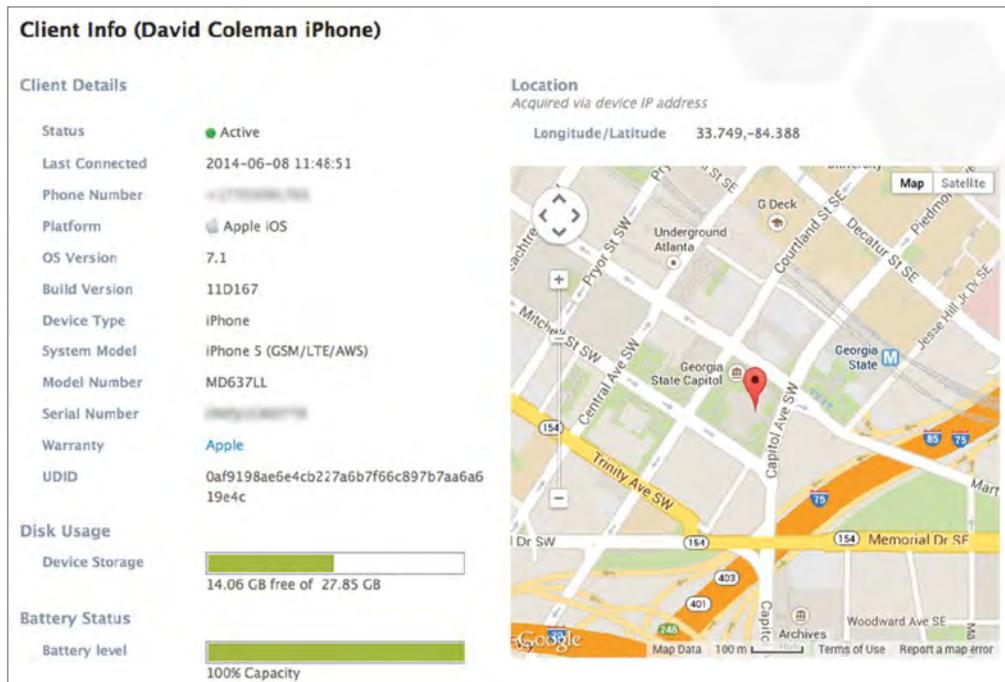
Сотрудник загружает MDM агент с публичного вебсайта или вебсайта компании, и устанавливает его на своем Android устройстве. MDM агент связывается с MDM сервером через БЛВС, и обычно требуется чтобы он аутентифицировался на сервере. MDM агент должен дать разрешение MDM серверу производить изменения на устройстве и работать в качестве администратора устройства. Когда это безопасная связь установлена, программа MDM-агент принудительно применяет ограничения устройства и конфигурационные изменения. MDM администрирование на Android устройстве осуществляется агентским приложением на устройстве. Изменения могут, однако, быть отправлены агентским приложением MDM с MDM сервера через сервис Облачных Сообщений Google [Google Cloud Messaging (GCM)].

Хотя устройства iOS не требуют программного MDM агента, некоторые MDM решения предлагают iOS MDM агенты. MDM агент на iOS устройстве мог бы потенциально посыпать информацию обратно на MDM сервер, которая не определена Apple APIs.

## Управление через эфир [Over-the-air management]

Когда устройство обеспечено настройками MDM сервером и зарегистрировано на нем, существует постоянная связь управления между MDM сервером и мобильным устройством. Как показано на Рисунке 18.9 MDM сервер может мониторить такую информацию об устройстве, как название, серийный номер, емкость, время жизни аккумуляторной батареи, и приложения, которые установлены на устройстве. Информация, которую нельзя посмотреть включает SMS сообщения, личная электронная почта, календарь, и история браузера.

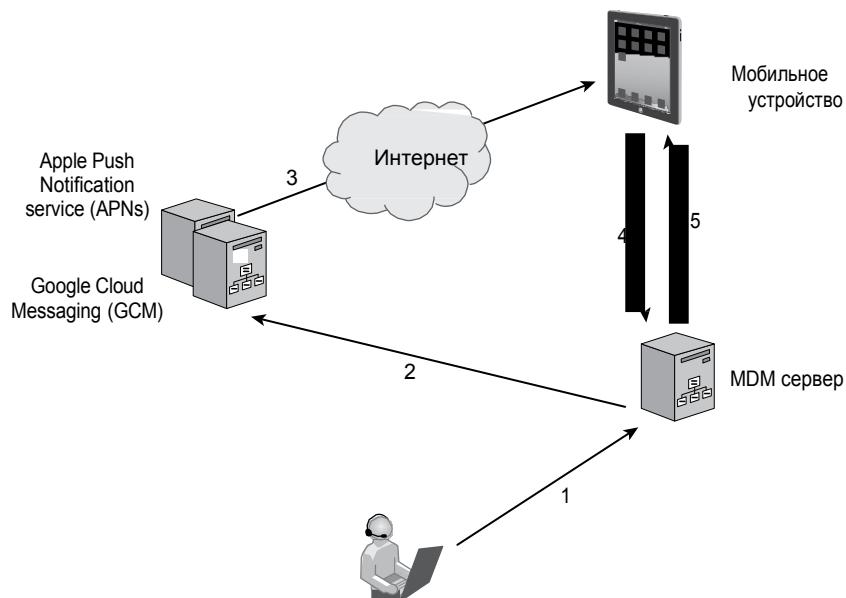
**РИСУНОК 18.9** Информация об устройстве



Мобильное устройство может все еще управляться удаленно, даже если мобильное устройство больше не подключено к корпоративной БЛВС. MDM сервер может продолжать управлять устройством, пока устройство подключено к Интернет в любом месте. Связь между MDM сервером и мобильными устройствами требует push уведомлений стороннего сервиса. И Google, и Apple имеют APIs, которые позволяют приложениям отправлять push уведомления на мобильные устройства. iOS приложения взаимодействуют с серверами сервиса Push Уведомлений Apple [Apple Push Notification service (APNs)], а приложения Android взаимодействуют с серверами Облачных Сообщений Google [Google Cloud Messaging (GCM)].

Как показано на Рисунке 18.10 первым шагом MDM администратора является внесение изменений в конфигурационный профиль MDM на MDM сервере. Затем MDM сервер связывается с серверами push уведомлений. Ранее установленное безопасное соединение уже существует между серверами push уведомлений и мобильным устройством. Сервис push уведомлений посыпает сообщение мобильному устройству с просьбой связаться с MDM сервером через Интернет. Когда мобильное устройство связывается с MDM сервером, MDM сервер посыпает изменения настроек и/или сообщения на мобильное устройство.

**РИСУНОК 18.10** Управление через эфир [Over-the-air management]



Какой тип удаленных действий через Интернет может выполнить администратор MDM?

- Сделать изменение настроек
- Сделать изменение ограничений устройства [device restrictions]
- Доставить сообщение на устройство

- Заблокировать устройство
- Стереть все с устройства
- Внести изменения в управление приложениями

### Стоп, Вор!

На украденном устройстве компании может быть удаленно все стерто. MDM производители применяют различные типы удаленной очистки [wipe].

**Корпоративная очистка [Enterprise Wipe]**      Стирает все корпоративные данные с выбранного устройства и удаляет устройство из MDM. Все корпоративные данные, содержащиеся на устройстве удаляются, включая MDM профили, политики и внутренние приложения. Устройство будет возвращено в состояние, в котором оно было до регистрации в MDM.

**Полная очистка устройства [Device Wipe]**      Стирает все данные с устройства, включая все данные, электронную почту, профили, и возможности MDM, и возвращает устройство в заводские настройки.

## Управление Приложениями

Корпоративные MDM решения также предлагают различные уровни управления приложениями, которые работают на мобильных устройствах. Когда установлен MDM профиль, все приложения, установленные на устройстве, можно посмотреть на MDM сервере, как показано на Рисунке 18.11. MDM сервер может управлять приложениями с помощью белых и/или черных списков конкретных приложений, которые могут использоваться на мобильных устройствах. Управление приложениями на устройствах компании является обычным делом; однако, управление приложениями на персональных устройствах сотрудников не так распространено.

MDM решения интегрированы с публичными магазинами приложений, такими как iTunes и Google Play, для того, чтобы разрешить доступ к публичным приложениям. MDM сервер взаимодействует с сервером push уведомлений, который затем размещает иконку приложения на мобильном устройстве. Пользователь мобильного устройства может затем установить приложение. Программа Объемной Закупки компании Apple [Apple Volume Purchase Program (VPP)] предоставляет предприятиям и образовательным институтам вариант приобретения приложений крупными партиями и распространения их по их организациям. Приложения могут быть приобретены и установлены в фоновом режиме на удаленные устройства. MDM сервер также может быть настроен на доставку приложения собственной разработки, которое может быть уникально для этой компании.

Как показано на Рисунке 18.12, электронные книги [eBooks] также могут управляться и распространяться на мобильные устройства через платформу MDM. Мы предлагаем, чтобы ваша компания осуществила объемную закупку электронной книги *CWNA Учебное Пособие [CWNA Study Guide eBook]*.

РИСУНОК 18.11 Приложения мобильного устройства

| Inventory | Management        | History                     |              |              |               |                   |             |              |
|-----------|-------------------|-----------------------------|--------------|--------------|---------------|-------------------|-------------|--------------|
|           |                   |                             | Name         | Version      | Short Version | Management Status | Bundle Size | Dynamic Size |
|           | General           | David Coleman's iPad        | AccuWeather  | 2.1.1        | 2.1.1         | Unmanaged         | 85 MB       | 8 MB         |
|           | Hardware          | iPad 4th Generation (Wi-Fi) | AwardWallet  | 2.3          |               | Unmanaged         | 9 MB        | 488 KB       |
|           | User and Location |                             | Calculator   | 1.3          | 1.3           | Unmanaged         | 19 MB       | 12 KB        |
|           | Purchasing        |                             | Chrome       | 34.0.1847.18 | 34.1847.18    | Unmanaged         | 48 MB       | 8 KB         |
|           | Security          | Data protection is enabled  | Educreations | 1377         | 1.5.5         | Unmanaged         | 12 MB       | 552 KB       |
|           | Apps              | 15 Apps                     | Expenses     | 8.2.5        | 8.2.5         | Unmanaged         | 46 MB       | 9 MB         |
|           | Network           |                             | Fly Delta    | 199          | 1.2           | Unmanaged         | 166 MB      | 31 MB        |
|           | Certificates      | 2 Certificates              | Hulu Plus    | 32000        | 3.2           | Unmanaged         | 18 MB       | 11 MB        |
|           | Profiles          | 4 Profiles                  | LinkedIn     | 7.0.1        | 81            | Unmanaged         | 43 MB       | 2 MB         |
|           |                   |                             | Netflix      | 2101571      | 5.2           | Unmanaged         | 30 MB       | 44 MB        |
|           |                   |                             | NYTimes      | 22057.216    | 3.0.1         | Unmanaged         | 15 MB       | 55 MB        |
|           |                   |                             | realtor.com  | 5.1.2.8798   | 5.1.2         | Unmanaged         | 30 MB       | 76 KB        |
|           |                   |                             | Twitter      | 5.11.1       | 5.11.1        | Unmanaged         | 20 MB       | 5 MB         |

РИСУНОК 18.12 Распространение электронной книги CWNA Study Guide eBook через MDM

The screenshot shows the MDM interface with the following details:

- Left sidebar:** Shows navigation options like Search Inventory, Configuration Profiles, Provisioning Profiles, Apps, eBooks, Smart Mobile Device Groups, Static Mobile Device Groups, Classes, Enrollment Profiles, Enrollment Invitations, and Management Settings.
- Top navigation bar:** Includes icons for Computers, Mobile Devices, Users, Notifications (with 1 notification), and a search bar.
- Central content area:**
  - Title:** CWNA Study Guide eBook
  - General tab:** Contains fields for Display Name (CWNA Study Guide eBook), Category (None), Distribution Method (Install Automatically/Prompt Users to Install (iOS only)), Make eBook managed when possible (checked), eBook URL (<https://itunes.apple.com/us/book/cwna-certified-wireless-network-administrator-official/>), and File Type (iBOOK).
  - Scope tab:** (This tab is partially visible in the screenshot.)

# Самостоятельная регистрация устройств для сотрудников

Как вы узнали MDM решения могут быть использованы для управления и обеспечения и БЛВС устройств компании, и БЛВС устройств сотрудников. Типовая настройка для управления устройствами сотрудников [BYOD] - это решение самостоятельной регистрации устройств [*self-service device onboarding*], а не надежный корпоративный MDM. Основная цель решения самостоятельной регистрации устройства - в предоставлении недорогого и простого способа обеспечения персональных БЛВС устройств сотрудников в безопасном корпоративном SSID. Решение самостоятельной регистрации устройств не означает предложения всех аспектов мониторинга и ограничений полноценного MDM. Вместо этого, решение по регистрации устройств предоставляет метод самообслуживания для сотрудников по настройке BYOD клиента и установки учетных данных безопасности, таких как корневой сертификат ЦС 802.1X/EAP [802.1X/EAP root CA certificate].

Рассмотрим этот сценарий: Джейф входит (logs in) в корпоративную сеть как сотрудник со своего корпоративного компьютера с помощью 802.1X/EAP. Его имя пользователя подтверждается базой данных LDAP с помощью RADIUS. В этом сценарии, Джейф является доверенным в качестве пользователя, так как его имя пользователя и пароль действительны. Его корпоративный ноутбук является доверенным, потому что его машина может быть подтверждена. Однако, Джейф использует свой корпоративный ноутбук по-другому, нежели чем как Джейф использует свой смартфон, как Джейф использует свой персональный ноутбук, или как Джейф использует свой планшет.

В реальном мире аутентификации и шифрования 802.1X/EAP обычно является требуемым методом для обеспечения защищенного доступа к корпоративной сети и данным. Однако, настройка клиента пользователя является не той задачей, которая может быть легко выполнена нетехническим пользователем. Кроме того, нужно, чтобы корневой сертификат ЦС [root CA certificate] был безопасно передан на клиентское устройство и установлен. Это может быть проблемой для корпораций и сотрудников-пользователей BYOD, так как корпорация не предоставляет доступ неправильно настроенному устройству. Как вы можете представить, размещение требуемого обученного сотрудника в ИТ поддержку для настройки персональных устройств сотрудников является не практичным. Решение - это процесс, который называется регистрация [*onboarding*].

Соответствующим образом настроенная и защищенная 802.1X/EAP сеть требует, чтобы корневой сертификат ЦС [root CA certificate] был установлен на клиенте. Установки корневого сертификата на ноутбуки с Windows могут быть легко автоматизированы с помощью *Объекта Групповых Политик* [*Group Policy Object (GPO)*], если ноутбук с Windows является участником домена Активного Каталога [*Active Directory (AD)*]]. Однако, GPO не может быть использован для macOS, iOS, мобильных устройств на Android, IoT устройств, или персональных BYOD устройств на Windows, которые не присоединены к домену AD. Ручная установка сертификатов на мобильные устройства, IoT устройства и устройства сотрудников является кошмаром администратора.

Решение по регистрации наиболее часто используется для установки корневых сертификатов ЦС [root CA certificates] на мобильные устройства, который будут использоваться с SSID с включенным 802.1X/EAP. Клиентские сертификаты также могут быть предоставлены решением по регистрации [*onboarding solution*]. Некоторые производители Wi-Fi, которые предлагают решения с динамическим PSK также предлагают

решения по регистрации, которые могут оснащать мобильные устройства клиентскими профилями Wi-Fi, настроенными с уникальными индивидуальными PSK.

Решения по самостоятельной регистрации для персональных устройств сотрудников может быть в различных формах и часто зависит от конкретного производителя БЛВС. Также доступны сторонние решения по самостоятельной регистрации, например: SecureW2 ([www.securew2.com](http://www.securew2.com)). Решения по регистрации обычно используют приложение, которое использует подходы в передаче настроек через эфир [over-the-air provisioning] аналогичные тем, что и решения MDM для безопасной установки сертификатов и клиентских Wi-Fi профилей на мобильные устройства. Решения по самостоятельной регистрации могут также использовать пользовательские приложения, созданные с помощью *программного интерфейса приложения* [*application programming interface (API)*] производителя БЛВС. Независимо от решения, регистрация устройств обычно требует начального подключения к БЛВС, чтобы завершить процесс самообслуживания.

## Регистрация с Двумя SSID

Регистрация с двумя SSID [Dual-SSID Onboarding] выполняется с использованием открытого SSID и защищенного 802.1X/EAP корпоративного SSID. Сотрудник сначала подключается к открытому SSID и направляется на страничку перехватывающего портала [captive portal]. В зависимости от того как реализована регистрация [onboarding] сотрудник может входить [log in] напрямую в перехватывающий портал [captive portal] с помощью корпоративных имени пользователя и пароля, или сотрудник может нажать на ссылку, которая перенесет его на экран входа системы регистрации, где он вводит свои имя пользователя и пароль. Аутентификация перехватывающего веб портала [captive web portal] проверяет действительность имени пользователя и пароля сотрудника через RADIUS и LDAP. Аутентификация через перехватывающий веб портал защищена HTTPSом.

После того как сотрудник вошел в сеть, обычно загружается приложение по регистрации [onboarding application] на мобильное устройство. Приложение по регистрации затем производит безопасную загрузку корневого сертификата 802.1X/EAP и/или других учетных данных безопасности, а также предоставляет информацию wi-fi клиенту [supplicant] на мобильном устройстве. Клиентские приложения по регистрации часто распространяются через открытый SSID. Решение по регистрации для разных типов пользователей также может быть доступно как веб приложение. Рисунок 18.13 показывает клиентское веб приложение по регистрации [onboarding web application], используемое Советом по Образованию в Калгари [Calgary Board of Education] для предоставления различных учетных данных безопасности гостям, студентам и персоналу.

После того как устройству сотрудника предоставлены все данные с помощью приложения регистрации, оно может подключаться к безопасной, т.е. защищенной сети. Так как безопасная сеть - это отдельный SSID, то сотруднику нужно будет вручную отключиться от открытого SSID и переподключиться к безопасному SSID.

## Регистрация с одним SSID

Регистрация с одним SSID [Single-SSID onboarding] использует один SSID, который способен аутентифицировать клиентов 802.1X/EAP- PEAP и клиентов 802.1X/EAP-TLS. Клиенты изначально входят [logs in] в SSID с использованием соединения 802.1X/EAP-PEAP, используя свои корпоративные имя пользователя и пароль. После того, как устройство вошло в сеть, сотрудник заходит на страничку перехватывающего портала [captive portal], требующего, чтобы пользователь снова вошел [log in], в этот раз для проверки, что ему разрешено пройти процесс регистрации. Также, как и Регистрацией с двумя SSID, загружается и запускается программа регистрации на устройство, и затем приложение загружает серверные сертификаты по SSL и необходимую информацию для Wi-fi клиента [supplicant] на устройстве.

После того, как устройство настроено, RADIUS сервер инициирует Изменение Авторизации [Change of Authorization (CoA)] для устройства сотрудника, отключая устройство от сети. Устройство немедленно переподключается к тому же самому SSID, используя или 802.1X/EAP-PEAP, или 802.1X/EAP-TLS, в зависимости от беспроводного профиля, который был установлен на устройство сотрудника. В этот раз клиент также проверяет действительность серверного сертификата.

**РИСУНОК 18.13** Приложение по регистрации устройств сотрудников [BYOD]  
Любезно предоставлено Советом по Образованию в Калгари [Calgary Board of Education]



## MDM или Самостоятельная Регистрация

MDM решения часто являются более предпочтительным выбором для больших корпораций. Корпоративные MDM дают корпорациям возможность управлять и отслеживать устройства БЛВС компаний, а также предоставляют решение по оснащению персональных БЛВС устройств сотрудников нужной информацией. Однако, MDM решение не всегда является лучшим выбором для BYOD решения. Корпоративные установки MDM часто имеют заградительную стоимость для предприятий среднего и малого бизнеса. Как ранее упоминалось, сотрудникам часто не нравится использовать MDM, из-за вопросов с приватностью.

Решения по самостоятельной регистрации устройств обычно более дешевое и проще для развертывания в качестве BYOD решения. Решения по самостоятельной регистрации используются в основном для предоставления необходимых данных БЛВС устройствам сотрудников, и не используются для принудительных ограничений устройства или для управления через эфир [over-the-air management]. Вопросы приватности более не являются проблемой для персональных устройств сотрудников.

В зависимости от требований безопасности компании, MDM, самостоятельная регистрация, или комбинация двух решений может быть выбрана для BYOD решения.

# Доступ в Гостевой БЛВС

Хотя основной целью для корпоративных БЛВС всегда было предоставление сотрудникам беспроводной мобильности, доступ к БЛВС для гостей компании может быть также важен. Заказчикам, консультантам, поставщикам и подрядчикам часто нужен доступ в Интернет, чтобы выполнить рабочие обязанности. Если они более продуктивны, то и сотрудники будут более продуктивны. Гостевой доступ также может быть добавляющим ценность сервисом [value-added service] и часто возвращает лояльность заказчиков. В сегодняшнем мире, бизнес заказчики ожидают получить гостевой Wi-Fi доступ. Свободный гостевой доступ часто рассматривается добавляющим ценность сервисом [value-added service]. Существует шанс, что ваши заказчики уйдут к конкурентам, если вы не предоставляете гостевой Wi-Fi доступ. Розничные сети, сети ресторанов, и сети отелей являются основными примерами сред, где беспроводной доступ в Интернет часто ожидается заказчиками.

Основная цель гостевого БЛВС заключается в предоставлении беспроводного шлюза в Интернет для посетителей и/или заказчиков компании. В целом, гостевым пользователям не нужен доступ к сетевым ресурсам компании. Следовательно, наиболее важный аспект безопасности гостевой БЛВС заключается в защите сетевой инфраструктуры компании от гостевых пользователей. В ранние дни Wi-Fi, гостевые сети были не очень распространены, из-за страха, что гостевые пользователи могут получить доступ к корпоративным ресурсам. Гостевой доступ часто предоставлялся на отдельной инфраструктуре. Еще одна типовая стратегия была в том, чтобы отправить весь гостевой трафик на отдельный шлюз, который отличался от Интернет шлюза для сотрудников компании. Например, для корпоративного шлюза могли использовать линии T1 (1544кбит/с) или T3(44736кбит/с), в то время как весь гостевой трафик шел по отдельным DSL телефонным линиям.

С годами доступ к гостевой БЛВС вырос в популярности, и различные типы решений гостевых БЛВС эволюционировали, чтобы удовлетворять потребностям. В следующих разделах мы обсудим аспекты безопасности гостевых БЛВС. Как минимум, должен быть отдельный гостевой SSID, уникальный гостевой VLAN, и гостевая политика межсетевого экрана. Дополнительно, мы обсудим использование перехватывающего веб портала [captive web portals] в гостевой БЛВС. Мы также обсудим множество опций гостевого доступа, которые доступны, включая гостевую самостоятельную регистрацию.

## Гостевой SSID

В прошлом, распространенная стратегия SSID была в разделении (сегментировании) разных типов пользователей—даже сотрудников—по отдельным SSID; каждый SSID был привязан к независимому VLANы. Например, в больнице могли быть уникальные пары SSID/VLAN для врачей, медсестер, техников и администраторов. Эта стратегия редко рекомендуется нынче, из-за служебной информации 2ого уровня, создаваемой несколькими SSID. Сегодня, более общепринятый метод заключается в размещении всех сотрудников в одном и том же SSID, и использованием атрибутов Службы Удаленной Аутентификации Пользователей по Телефонным Подключениям [Remote Authentication Dial-In User Service (RADIUS)] для назначения разным группам пользователей разных VLANов. Что не изменилось со временем - это рекомендация, чтобы весь трафик гостевых пользователей помещался в отдельный SSID. Гостевой SSID будет всегда иметь отличные параметры безопасности от SSID для сотрудников, поэтому

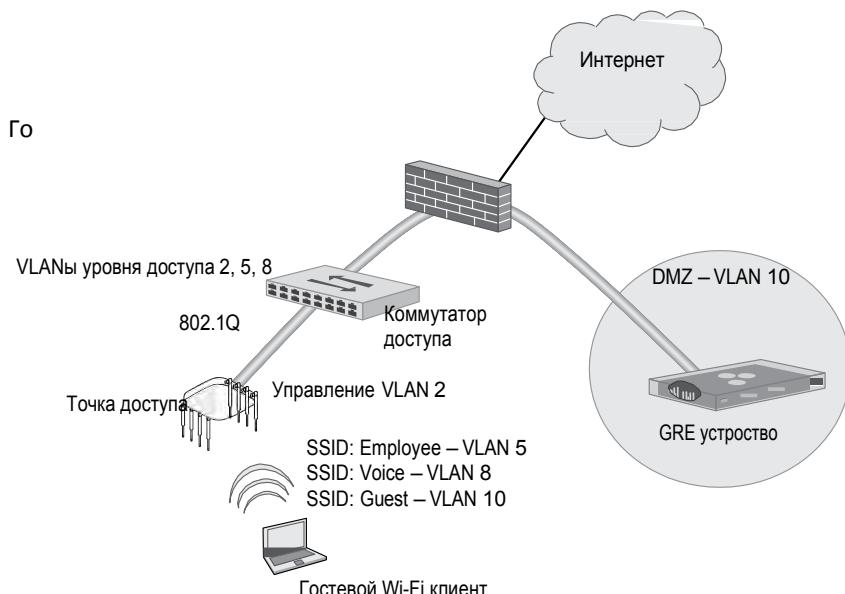
сохраняется необходимость в отдельном гостевом SSID. Например, SSID сотрудников обычно защищены безопасностью 802.1X/EAP, в то время как гостевые SSID наиболее часто являются открытыми сетями, которые используют перехватывающий веб портал [captive web portal] для аутентификации. Хотя шифрование обычно не предоставляется для гостевых пользователей, некоторые производители БЛВС начали предлагать шифрованный гостевой доступ и обеспечивать конфиденциальность данных с использованием уникальных учетных данных PSK на каждого пользователя или на каждое устройство. Шифрованный гостевой доступ также может быть предоставлен с 802.1X/EAP с Хотспот 2.0 [Hotspot 2.0] для клиентских устройств с поддержкой Пасспоинт [Passpoint], которая обсуждается позже.

Как и все SSID, гостевой SSID никогда не должен быть скрыт и должен иметь простое наименование, например как CWNA-Guest. В большинстве случаев, гостевой SSID в первую очередь показан на табличке в вестибюле(лобби) или входе в офисы компаний.

## Гостевой VLAN

Гостевой пользовательский трафик должен быть помещен в уникальный VLAN, связанный с IP подсетью, которая не смешивается с VLANами сотрудников. Отделение ваших гостевых пользователей в уникальный VLAN является передовым опытом безопасности и управления. Основные дебаты о гостевом VLANе в том должен ли он поддерживаться на границе сети. Как показано на Рисунке 18.14, частый проектный сценарий в том, что гостевой VLAN не существует на краю сети, а вместо этого является изолированным, в так называемой демилитаризованной зоне [*demilitarized zone (DMZ)*]. Как изображено на Рисунке 18.14, гостевой VLAN (VLAN 10) не существует на уровне доступа; следовательно, весь гостевой трафик должен быть туннелирован от ТД до DMZ, где существует гостевой VLAN. IP туннель, обычно использующий протокол Универсальной Маршрутизирующей Инкапсуляцией [Generic Routing Encapsulation (GRE)], транспортирует гостевой трафик с границы сети до изолированного DMZ. В зависимости от решения производителя БЛВС, точкой назначения туннеля в DMZ может быть контроллер БЛВС, сервер GRE, или маршрутизатор.

**РИСУНОК 18.14** GRE туннелирование гостевого трафика в DMZ



Хотя изоляция гостевого VLAN в DMZ была обычной практикой многие годы, это больше не нужно, если гостевые политики межсетевого экрана применены на границе сети. Различные производители БЛВС теперь встраивают корпоративного уровня межсетевые экраны в точки доступа. Если гостевая политика межсетевого экрана может быть применена на границе сети, гостевой VLAN может также располагаться на коммутаторе доступа и туннелирование будет не нужно.

## Гостевые политики межсетевого экрана

Наиболее важный компонент безопасности гостевого БЛВС - это политика межсетевого экрана. Политика межсетевого экрана гостевой БЛВС предотвращает прохождение трафика гостевых пользователей рядом с сетевыми ресурсами и инфраструктурой компании. Отделение гостевого трафика от трафика сотрудников является критичным. Рисунок 18.15 показывает очень простую гостевую политику межсетевого экрана, которая разрешает DHCP и DNS, но запрещает доступ к частным сетям 10.0.0.0/8, 172.16.0.0/12, и 192.168.0.0/16. Гостевые пользователи не разрешены на этих частных сетях, так как корпоративные сетевые сервера и ресурсы часто располагаются на этом частном IP пространстве. Гостевая политика межсетевого экрана должна просто маршрутизировать весь гостевой трафик прямо на Интернет шлюз и прочь из корпоративной сетевой инфраструктуры.

**РИСУНОК 18.15** Гостевые политики межсетевого экрана

| Source IP | Destination IP          | Service     | Action |
|-----------|-------------------------|-------------|--------|
| Any       | Any                     | DHCP-Server | PERMIT |
| Any       | Any                     | DNS         | PERMIT |
| Any       | 10.0.0.0/255.0.0.0      | Any         | DENY   |
| Any       | 172.16.0.0/255.240.0.0  | Any         | DENY   |
| Any       | 192.168.0.0/255.255.0.0 | Any         | DENY   |
| Any       | Any                     | Any         | PERMIT |

Порты межсетевого экрана, которые должны быть разрешены включают DHCP сервер (UDP порт 67), DNS (UDP порт 53), HTTP (TCP порт 80), и HTTPS (TCP порт 443). Это позволит беспроводным устройствам гостевых пользователей получать IP адреса, осуществлять DNS запросы, и бороздить веб. Многие компании требуют, чтобы их сотрудники использовали безопасное VPN соединение, когда они подключаются к SSID, отличном от SSID компании. Следовательно, рекомендуется, чтобы IPsec IKE (UDP порт 500) и IPsec NAT-T (UDP порт 4500) также были разрешены.

Политика межсетевого экрана, показанная на Рисунке 18.15 представляет минимальную защиту, необходимую для гостевой БЛВС. Гостевая политика межсетевого экрана может быть более ограничивающей. В зависимости от политики компании, намного больше портов может быть заблокировано. Одна из практик - это форсировать использование вебпочты [webmail] для гостевых пользователей и блокировать SMTP и другие порты электронной почты так, чтобы пользователи не могли рассыпать спам [“spam”] через гостевую БЛВС. Однако, теперь большинство почтовых сервисов использует SSL, поэтому эта практика не так уж распространена. Это вопрос политики безопасности компаний, определить какие порты нужно

**868** Глава 18 • Приноси Свое Собственное Устройство (BYOD) и Гостевой Доступ заблокировать в гостевом VLANe. Если политика запрещает использовать SSH в гостевой БЛВС, то TCP порт 22 нужно будет заблокировать. В дополнение к блокировке UDP и TCP портов, у нескольких производителей БЛВС теперь есть возможность блокировать приложения. В дополнении к возможностям межсетевого экрана с контролем состояний, производители БЛВС начали встраивать межсетевые экраны уровня приложений с возможностью глубокой инспекции пакета [*deep packet inspection (dpi)*] в точке доступа или контроллеры БЛВС. Межсетевые экраны уровня приложений могут блокировать определенные приложения или группу приложений. Например, некоторые популярные приложения потокового видео могут быть заблокированы в гостевом SSID, как показано на Рисунке 18.16. Политика безопасности компании также будет определять какие приложения должны быть заблокированы или ограничены по скорости в гостевой БЛВС.

**РИСУНОК 18.16** Политика межсетевого экрана для приложений

| Source IP | Destination IP | Service              | Action |
|-----------|----------------|----------------------|--------|
| Any       | Any            | YOUTUBE              | DENY   |
| Any       | Any            | NETFLIX VIDEO STREAM | DENY   |
| Any       | Any            | FACETIME             | DENY   |
| Any       | Any            | GOOGLE VIDEO         | DENY   |
| Any       | Any            | INSTAGRAM VIDEO      | DENY   |
| Any       | Any            | Any                  | PERMIT |

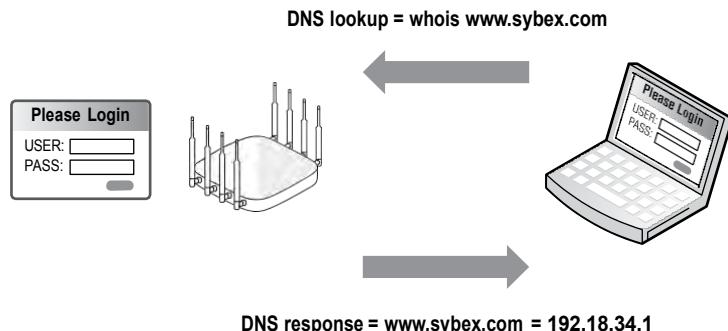
## Перехватывающие Веб Порталы

Часто, гостевые пользователи должны войти [*log in*] через страницу перехватывающего веб портала [*captive web portal page*] прежде, чем им будет дан доступ в Интернет. Вы вероятно пользовались перехватывающими веб порталами [*captive web portal*] когда входили [*logging*] в Wi-Fi в аэропортах или отелях. Один из наиболее важных аспектов страницы перехватывающего веб портала - это юридический отказ от ответственности [*legal disclaimer*]. Хороший юридический отказ от ответственности информирует гостевого пользователя о приемлемом поведении при использовании гостевой БЛВС. Предприятия скорее всего будут юридически защищены, если что-нибудь плохое, например, заражение компьютерным вирусом, произойдет с БЛВС устройством гостевого пользователя, пока он подключен через портал.

Решение *перехватывающего портала* [*captive portal*] фактически вовлекает веб браузер в сервис аутентификации. Чтобы аутентифицироваться, пользователь должен сначала подключиться к БЛВС и запустить веб браузер. После того как браузер запущен и пользователь попытался зайти на вебсайт, не важно какую веб страницу пользователь пытается открыть, пользователь перенаправляется на другой URL, который показывает страницу входа перехватывающего портала. Перехватывающие порталы могут перенаправить неаутентифицированных пользователей на страницу входа [*login page*] используя IP перенаправление, перенаправление DNS, или перенаправление по HTTP. Как показано на Рисунке 18.17 многие перехватывающие веб порталы запускаются DNS перенаправлением. Гостевой пользователь пытается открыть веб страницу, но DNS запрос перенаправляет браузер на IP адрес перехватывающего веб портала.

Перехватывающие порталы доступны как отдельные серверные решения или как облачный сервис. Кроме того, большинство производителей предлагают решения интегрированного перехватывающего портала. Перехватывающий портал может существовать в контроллере БЛВС, или может быть развернут на границе в точке доступа. Производители БЛВС, которые поддерживают перехватывающие порталы предоставляют возможность по настройке

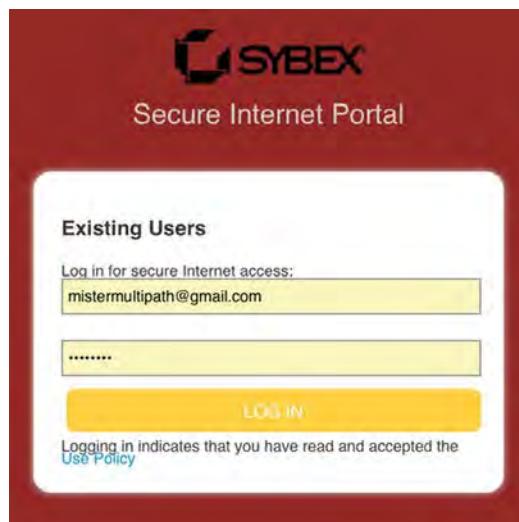
РИСУНОК 18.17 Перехватывающий веб портал—перенаправление DNS



страницы перехватывающего портала. Обычно вы можете персонализировать страницу путем добавления графики, например, логотип компании, вставки приемлемой политики использования, или настройки требований к логину [login]. Корпоративные предприятия также могут создавать перехватывающие веб порталы разного действия для разных типов пользователей, а также настраиваемые перехватывающие веб порталы для разных бизнес локаций.

В зависимости от выбранной безопасности гостевой БЛВС, могут использоваться разные типы страниц входа [login pages] перехватывающих веб порталов. Страница входа [login page] аутентификации пользователя требует, чтобы ТД или контроллер БЛВС запросил RADIUS сервер про гостевые имя пользователя и пароль. Если у гостя еще нет учетной записи, то страница входа может предоставить ссылку, позволяющую пользователю создать гостевую учетную запись, как показано на Рисунке 18.18. Страница регистрации гостя позволяет пользователю ввести необходимую информацию про себя для самостоятельной регистрации, как показано на Рисунке 18.19. Гостевой пользователь может также быть подключен к веб странице перехватывающего портала, требующей от него просто подтверждения соглашения о принятии пользовательской политики, как показано на Рисунке 18.20.

РИСУНОК 18.18 Перехватывающий веб портал—гостевой вход



**РИСУНОК 18.19** Перехватывающий веб портал—самостоятельная регистрация гостя

**Guest Registration**

Please complete the form below to gain access to the network.

**Visitor Registration**

\* Your Name: David Westcott  
Please enter your full name.

Phone Number: 555-123-4567  
Please enter your contact phone number.

\* Company Name: Westcott Consulting, Inc.  
Please enter your company name.

\* Email Address: david@westcott-consulting.com  
Please enter your email address.  
This will become your username to log into the network.

\* Confirm:  I accept the terms of use

**Register**

\* required field

Already have an account? [Sign In](#)

**РИСУНОК 18.20** Перехватывающий веб портал—принятие политики

Welcome to our Internet portal. If you choose to continue, you are agreeing to comply with and be bound by the following terms and conditions of use. If you disagree with any part of these terms and conditions, you may not continue.

**Terms of use:**

- Your use of any information or materials on sites you access is entirely at your own risk, for which we shall not be liable.
- You agree that, though this portal, you will not perform any of the following acts:
  - Attempt to access devices or resources to which you have no explicit, legitimate rights
  - Copy, reproduce, or transmit any copyrighted files or information other than in accordance with the requirements and allowances of the copyright holder
  - Launch network attacks of any kind including port scans, DoS/DDoS, packet floods, replays or injections, session hijacking or interception, or other such activity with malicious intent
  - Transmit malicious software such as viruses, Trojan horses, and worms
  - Surreptitiously install software or make configuration changes to any device or application, by means of the installation or execution of key loggers, registry keys, or other executable or active application or script
- You agree that you will use the access provided here responsibly and with full regard to the safety, security, and privacy of all other users, devices, and resources.
- You agree that you will be mindful of the cultural sensitivities of others while using this portal so as not to provoke reaction or offense, and that you will not intentionally access pornographic, graphically violent, hateful, or other offensive material (as deemed by us) regardless of others' sensitivities.
- You understand that we reserve the right to log or monitor traffic to ensure that these terms are being followed.
- You understand that unauthorized use of resources through this portal may give rise to a claim for damages and/or be a criminal offense.

**ACCEPT**      **DECLINE**

RADIUS серверы часто используются с аутентификацией перехватывающего портала для подтверждения учетных данных гостевого пользователя для гостевого SSID. Решение перехватывающего веб портала делает запрос к RADIUS серверу про имя пользователя и пароль с использованием слабого протокола аутентификации, такого как MS-CHAPv2. В отличии от использования уже существующей базы данных пользователей, такой как Активный Каталог [Active Directory], гостевые учетные данные обычно создаются во время процесса регистрации гостя, и часто хранятся в родной базе данных RADIUS сервера. Аутентификация перехватывающего веб портала также часто используется совместно с решениями BYOD для подтверждения учетных данных сотрудников. В этом случае, база данных сотрудников вероятнее всего будет Активным Каталогом [Active Directory], которая в свою очередь будет опрашиваться RADIUS сервером.

Держите в уме, что перехватывающий веб портал [captive web portal] требует взаимодействия с пользователем, и иногда впечатления гостевого пользователя могут стать негативными. Перехватывающие веб порталы часто не срабатывают после обновлений браузера или обновлений операционной системы мобильного устройства. Проблемы с DNS также являются причиной неработоспособности перехватывающего веб портала. Более того, дизайн многих перехватывающих веб порталов не всегда дружественен пользователю.

Дополнительно, производители смартфонов, такие как Apple и Samsung разрабатывают более сложные методы рандомизации MAC адресов в своих устройствах. Рандомизация MAC применяется производителями смартфонов как средство решения проблем с конфиденциальностью. Однако, статус авторизации на перехватывающем веб портале обычно привязывается к MAC адресу зарегистрированного устройства. В зависимости от частоты рандомизации (т.е. изменения случайным образом) MAC адреса, гостевые пользователи могут быть вынуждены проходить повторную аутентификацию через перехватывающий веб портал много раз.

В какое-то время почти каждый имел неудачный опыт с перехватывающим веб порталом. Перехватывающие веб порталы должны иметь простой дизайн, должны быть просты к пониманию, и тщательно протестированы, чтобы обеспечить наилучшие впечатления гостевому пользователю.

## Изоляция клиентов, ограничение скорости, и фильтр содержимого веб

Когда гостевые пользователи подключены к гостевому SSID, они все находятся в одном и том же VLANe в одной и той же IP подсети. Так как они находятся в одном и том же VLANe, гости могут проводить атаки равный-с-равным [peer-to-peer attacks] против друг друга. Изоляция клиентов [Client isolation] - это функция, которая может быть включена на БЛВС точках доступа или контроллерах, чтобы блокировать беспроводных клиентов от прямого взаимодействия с другими беспроводными клиентами в одном и том же беспроводном VLANe. *Изоляция клиентов [Client isolation]* (или другие различные термины, используемые для описания этой функции) обычно означает, что пакеты, прибывающие на беспроводной интерфейс ТД, не разрешено пересыпать обратно в беспроводной интерфейс другим клиентам. Это изолирует каждого пользователя на беспроводной сети, чтобы гарантировать, что беспроводная станция не может быть использована для получения доступа уровня 3 или выше к другим беспроводным станциям. Функция изоляции клиентов обычно является конфигурируемой настройкой на каждый SSID, связанный с уникальным VLAN. Изоляция клиентов настоятельно рекомендуется в гостевых БЛВС для предотвращения атак равный-с-равным [prevent peer-to-peer attacks].

Производители корпоративных БЛВС также предлагают сжать полосу пользовательского

**872** Глава 18 • Приноси Свое Собственное Устройство (BYOD) и Гостевой Доступ трафика. *Сжатие полосы [Bandwidth throttling]*, также называется *ограничение скорости [rate-limiting]*, может использоваться для сдерживания трафика или на уровне SSID, или на уровне пользователя. Ограничение скорости [Rate limiting] часто применяется в гостевых БЛВС. Это может гарантировать, что основная полоса будет зарезервирована для сотрудников. Ограничение скорости гостевого пользовательского трафика в 1024кбит/с является обычной практикой. Однако, так как гостевой доступ обычно рассматривается как добавляющий ценность сервис [value-added service], ограничение скорости на гостевом SSID может оказаться не очень хорошей стратегией.

Некоторые предприятия, которые пытаются монетизировать доступ к гостевому БЛВС, часто предоставляют два уровня гостевого доступа. Свободный уровень гостевого доступа - ограничен по скорости, в тоже время платный гостевой доступ не имеет ограничений по полосе.

Корпоративные предприятия часто разворачивают решения по фильтрации веб содержимого [*web content filter*], чтобы ограничить типы вебсайтов, которые их сотрудники могут просматривать на рабочем месте. Решение по фильтрации веб содержимого блокирует сотрудников от просмотра вебсайтов на основе категории содержимого. Каждая категория содержит вебсайты или веб страницы, которые включаются в категорию на основе их основного содержимого. Например, компания может использовать фильтр веб содержимого для блокировки сотрудников от просмотра любых вебсайтов, которые имеют отношение к азартным играм или насилию. Фильтрация содержимого наиболее часто используется для блокировки того, что могут сотрудники просматривать в Интернете, но фильтрация содержимого также может быть использована для блокировки определенных типов вебсайтов для гостевых пользователей. Весь гостевой трафик может быть смаршрутизирован через фильтр веб содержимого компании.

## Управление Гостями

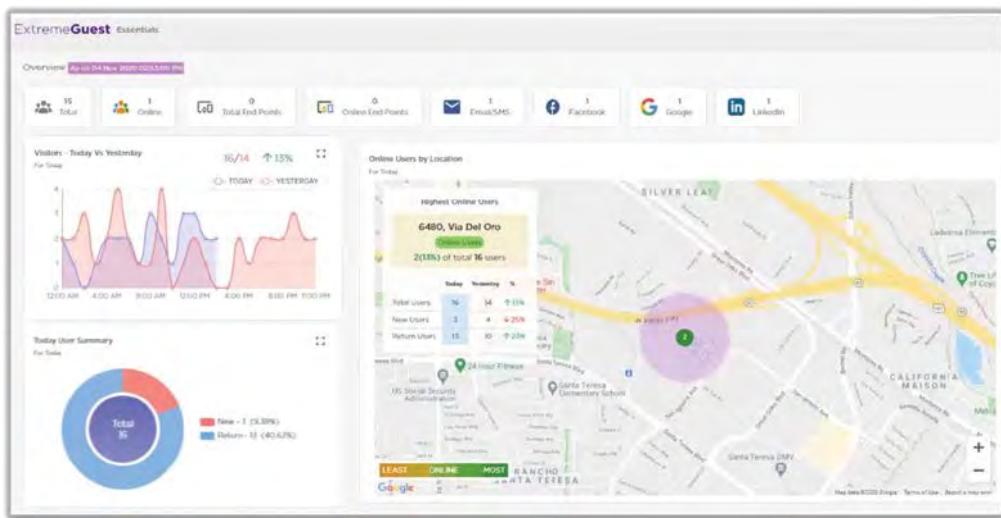
По мере развития Wi-Fi, развивались и решения для управления гостями БЛВС. Большинство гостевых БЛВС требует от гостевых пользователей аутентифицироваться с учетными данными через перехватывающий веб портал. Следовательно, должна быть создана база данных с пользовательскими учетными данными. В отличие от пользовательских учетных записей в уже существующей базе данных Активного Каталога [Active Directory], гостевые пользовательские учетные записи обычно создаются на лету и в отдельной базе данных гостевых пользователей.

Информация о гостевом пользователе обычно собирается, когда гости прибывают в офисы компании. Кто-то должен отвечать за управление базой данных и создание учетных записей гостевых пользователей. ИТ администраторы обычно очень заняты, чтобы управлять гостевой базой данных; следовательно, сотрудник, который управляет базой данных - это часто секретарь в приемной или персона, которая встречает гостей на входе. Этому сотруднику требуется административная учетная запись к системе управления гостями, которые могут быть RADIUS сервером или каким-либо другим типом серверов гостевой базы данных. Администраторы управления гостями имеют права доступа для создания учетных записей гостевых пользователей в гостевой базе данных и выпускать гостевые учетные данные, которые обычно являются именем пользователя и паролем.

Сервер гостевого управления может быть облачным или располагаться на собственных серверах компании в data-центре компании. Хотя большинство систем управления гостями построены на основе RADIUS сервера, решения управления гостями предлагают функции в дополнение к предоставлению сервисов RADIUS. Современные решения управления гостями предлагают надежные возможности создания отчетов для аудита и соответствия требованиям. Решение управления гостями также может быть использовано как непрерывное 24/7 мониторинговое решение. Всестороннее решение управление гостями часто используется менеджерами розничных продаж, операторы объектов массовых мероприятий и гостиничного бизнеса для аналитического обзора поведения заказчиков. Например, сколько заказчиков входит в магазин, как часто они посещают магазин, и сколько времени в нем проводят - все это является параметрами, которые можно измерить. Как показано на Рисунке 18.21, гостевая аналитика поведения заказчиков может быть использована для улучшения привлечения заказчиков и расширения показа бренда.

ИТ администратор обычно настраивает решение управления гостями в самом начале; однако, секретарь компании будет иметь ограниченные права доступа для управления гостевыми пользователями. Решения управления гостями также могут быть интегрированы с LDAP для поручительства (или спонсорства) сотрудников, и обычно имеют некоторые варианты для самостоятельной регистрации гостевых пользователей. Наиболее часто решения управления гостями используется для беспроводных гостей, но они могут быть использованы и для аутентификации гостей в проводной части.

РИСУНОК 18.21 Аналитика Гостевого Wi-Fi



Как вы можете видеть на Рисунке 18.22, может быть несколько способов передачи учетных данных гостевому пользователю. Учетные данные [credentials] могут быть предоставлены через электронный кошелек [electronic wallet], текстовое сообщение SMS, сообщение электронной почты, или напечатанную квитанцию. SMS, электронная почта, квитанция также могут быть дополнены информацией о компании. Страница входа для регистрации гостей может быть вся настроена с размещением логотипа компании и информации о компании.

## Самостоятельная регистрация гостей

Решения управления гостями традиционно полагаются на секретаря компании или представителя в лобби для регистрации гостевых пользователей. Хорошее решение по гостевому управлению позволяет секретарю зарегистрировать одного пользователя или группу пользователей. За последние несколько лет был огромный толчок для гостевых пользователей создавать свои собственные учетные записи, что обычно называется самостоятельная регистрация [*self-registration*]. Когда гостевые пользователи перенаправляются на перехватывающий веб портал, если у них еще нет гостевой учетной записи, то ссылка на веб странице входа перенаправит их на страницу самостоятельной регистрации. Простые страницы самостоятельной регистрации позволяют гостям заполнить форму, и их гостевая учетная создается и отображается или распечатывается для них. Более продвинутые страницы самостоятельной регистрации требуют от гостя ввести адрес электронной почты или номер для SMS, который затем используется системой регистрации для отправки пользователю его учетных данных входа.

Как показано на Рисунке 18.23, некоторые решения управления гостями теперь предлагают приложения для киосков, где страница регистрации для входа работает на планшете, который работает как киоск. Самостоятельная регистрация через киоск очень полезна, когда киоск установлен в основном лобби или входе компании. Преимущество киосков самостоятельной регистрации в том, что секретарю не нужно помогать пользователям и можно сосредоточиться на других обязанностях.

РИСУНОК 18.22 Методы предоставления гостевых учетных данных

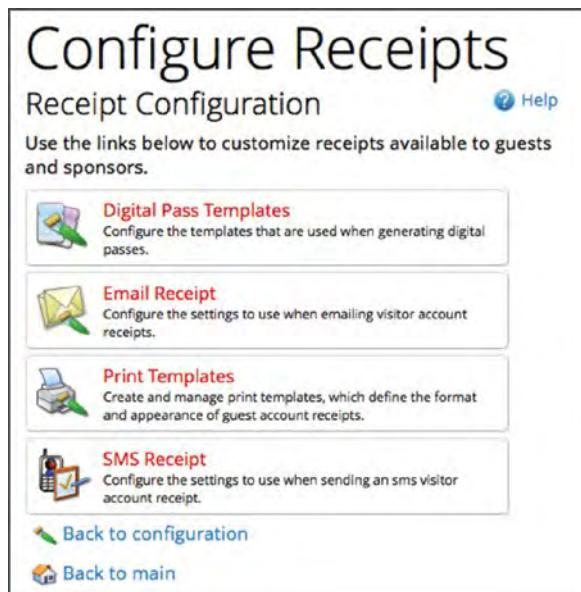


РИСУНОК 18.23 Киоск гостевого доступа

Любезно предоставлено КлаудКарие [CloudCarrier]



## Поручительство Сотрудников

От гостевых пользователей также может быть затребован ввод адреса электронной почты сотрудника, кто в свою очередь должен подтвердить и поручиться за гостя. Поручитель [sponsor] обычно получает сообщение электронной почты с ссылкой, которая позволяет ему просто принять или отклонить гостевой запрос. Когда пользователь зарегистрирован или спонсирован, он может войти с помощью своих вновь созданных учетных данных. Решение по управлению гостями с возможностью поручительства сотрудниками [*employee sponsorship*] могут быть интегрированы с базой данных LDAP, такой как Активный Каталог [Active Directory].

Как вы уже знаете, секретарь может зарегистрировать гостевых пользователей, или компания может выбрать использование киоска регистрации, чтобы гости могли самостоятельно регистрироваться. Для больших и распределенных организаций центральный регистрационный киоск не очень хорошо масштабируется. Самостоятельная регистрация с поручительством сотрудников становится популярной для многих организаций.

Когда гостевые пользователи изначально подключаются к гостевой сети, они перенаправляются на страницу перехватывающего портала. Страница перехватывающего портала предлагает им войти, если у них уже есть учетная запись, или она позволяет им нажать на ссылку, которая позволяет им создать свою собственную учетную гостевую запись [guest account]. Как показано на Рисунке 18.24, гость должен ввести адрес электронной почты сотрудника, который поручается [sponsoring] за него. Обычно, у гостей деловая встреча с сотрудником, который предоставляет поручительство [sponsorship].

**РИСУНОК 18.24** Регистрация с поручительством сотрудника

**Guest Registration**

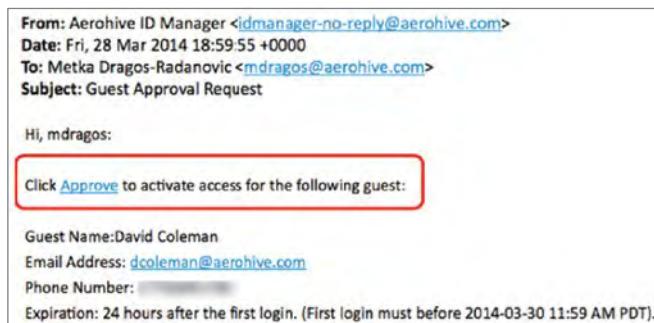
Please complete the form below to gain access to the network.

| Visitor Registration                             |                                                                                                                      |
|--------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|
| * Your Name:                                     | David Coleman<br>Please enter your full name.                                                                        |
| Phone Number:                                    | 555-123-4567<br>Please enter your contact phone number.                                                              |
| * Email Address:                                 | dcoleman@aerohive.com<br>Please enter your email address.<br>This will become your username to log into the network. |
| * Sponsor's Name:                                | Metka Dragos-Radanovic<br>Name of the person sponsoring this account.                                                |
| * Sponsor's Email:                               | mdragos@aerohive.com<br>Email of the person sponsoring this account.                                                 |
| * Confirm:                                       | <input checked="" type="checkbox"/> I accept the <a href="#">terms of use</a>                                        |
| <b>Register</b>                                  |                                                                                                                      |
| * required field                                 |                                                                                                                      |
| Already have an account? <a href="#">Sign In</a> |                                                                                                                      |

Когда форма регистрации заполнена и отправлена, поручитель [sponsor] получает электронную почту, уведомляющую его, что гость хотел бы получить сетевой доступ. Как показано на Рисунке 18.25, обычно сообщение электронной почты содержит ссылку, которую должен нажать поручитель [sponsor], чтобы подтвердить предоставление сетевого доступа.

Когда ссылка нажата, гостевая учетная запись подтверждается, и гость получает подтверждение, или по электронной почте или SMS, и ему дальше разрешено войти в сеть. Если поручитель не нажмет на ссылку, то гостевая учетная запись не создаться, и гостю будет отказано в доступе к сети.

**РИСУНОК 18.25** Электронное письмо с запросом подтверждения при поручительстве сотрудником.

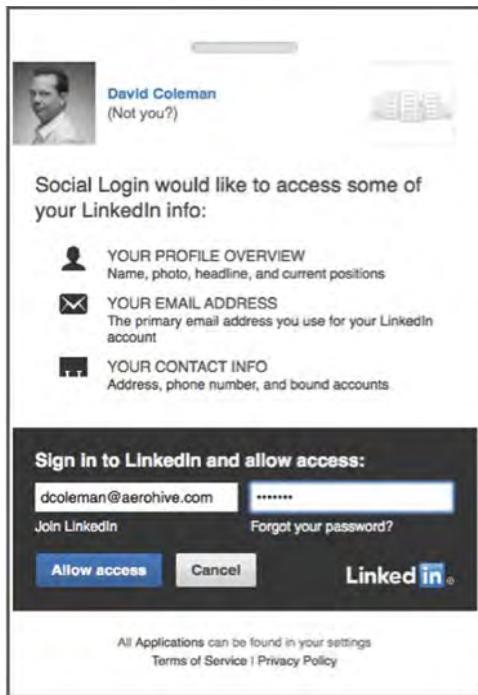
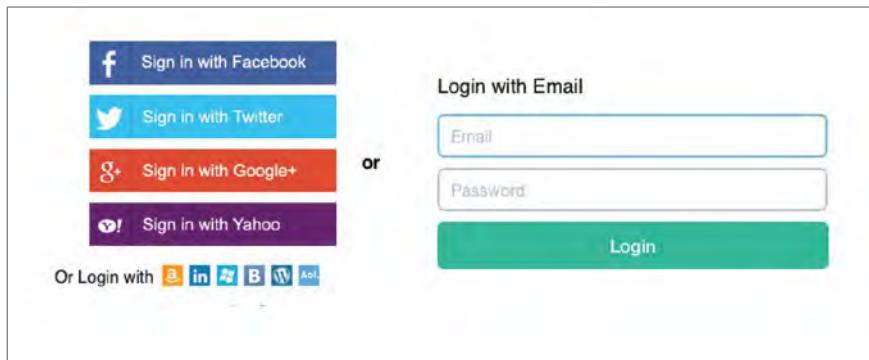


Поручительство сотрудниками гарантирует, что только авторизованному гостевому пользователю разрешена гостевая БЛВС, и что сотрудники компании активно вовлечены в процесс авторизации гостевых пользователей.

## Логин Социальной Сети

Новая тенденция в гостевых сетях в рознице и сфере услуг - это логин социальных сетей [*social login*]. Логин социальных сетей - это способ использования существующих учетных данных входа от социальных сетей (таких как Twitter, Facebook, или LinkedIn) для регистрации на сторонних вебсайтах. Логин социальных сетей позволяет пользователю отказаться от процесса создания новых регистрационных учетных данных для стороннего вебсайта. Логин социальных сетей часто включается с помощью протокола *OAuth*. OAuth - сокращение от английского Open Standard for Authorization [Открытый Стандарт Авторизации] - является безопасным протоколом авторизации, который разрешает серверу авторизации выпуск жетонов доступа [access tokens] сторонним клиентам. Как показано на Рисунке 18.26, структура авторизации OAuth 2.0 позволяет сторонним приложениям получить ограниченный доступ к сервису HTTP, и может быть использована для логина социальных сетей для гостевых Wi-Fi сетей.

Как показано на Рисунке 18.27, логин социальных сетей может быть связан с открытым гостевым SSID. Гостевые пользователи перенаправляются на страницу перехватывающего веб портала, где они могут затем войти в гостевую БЛВС с помощью своих существующих учетных данных входа в социальные среды. Предприятиям розничной торговли и сферы услуг нравится идея логина социальных сетей, потому что она позволяет им получить значимую маркетинговую информацию о гостевых пользователях из социальных сетей. Аналитика, встроенная в системы гостевого управления часто в значительной степени полагается на информацию, собранную с помощью логина социальных сетей. Далее предприятия могут создать базу данных о типах заказчиков, которые используют гостевой Wi-Fi во время покупок в магазине. Стоит отметить, что существуют некоторые юридические вопросы по поводу конфиденциальности, и входной перехватывающий веб портал всегда содержит юридический отказ от ответственности, гласящий, что информация о заказчике может быть собрана, если заказчик согласился использовать логин социальных сетей при регистрации в гостевой БЛВС.

**РИСУНОК 18.26** Приложение OAuth 2.0**РИСУНОК 18.27** Логин Социальной сети

## Шифрованный Гостевой Доступ

Большинство гостевых сетей являются открытыми сетями, которые не используют шифрование; таким образом, для гостевых пользователей нет конфиденциальности данных. В Главе 16, "Беспроводные Атаки, Мониторинг Вторжения и Политика" вы узнали о многочисленных атаках, которые делают незащищенных Wi-Fi пользователей уязвимыми.

Так как большинство гостевых БЛВС не используют шифрование, гостевые пользователи - это низко-висящий фрукт и, часто являются целью опытных хакеров или атакующих. По этой причине, многие корпорации требуют, чтобы их сотрудники использовали решения VPN, когда подключаются к любому виду публичных или открытых гостевых SSID. Так как гостевой SSID не предоставляет защиту данных, гостевые пользователи должны использовать свою собственную защиту в форме VPN соединения, которое обеспечивает шифрование и конфиденциальность данных.

Проблема в том, что многие потребители и гостевые пользователи не очень понимают, как использовать решение VPN, когда подключаются к открытой гостевой БЛВС. В результате, одна из недавних тенденций – обеспечивать шифрование и лучшую аутентификационную безопасность для гостевых Wi-Fi пользователей. Защита сетевой инфраструктуры компании от атак от гостевых пользователей все еще остается высшим приоритетом защиты. Однако, если компания также может обеспечить шифрование гостевого SSID, защита, предоставленная гостевым пользователям, является услугой, добавляющей ценность.

Один простой способ обеспечения шифрования на гостевом SSID – это использование статического PSK. Хотя шифрование, предоставляемое при использовании статического PSK, не идеально из-за усиленных атак перебора по словарю и атак социальной инженерии. Некоторые производители БЛВС предлагают облачные решения по распространению гостевых учетных данных безопасности в форме уникального PSK на каждого пользователя. Решение управления гостями, которое использует уникальные PSK в качестве аутентификационных учетных данных также обеспечивает конфиденциальность данных для гостевых пользователей с шифрованием WPA2.

## Хотспот 2.0 и Пасспоинт

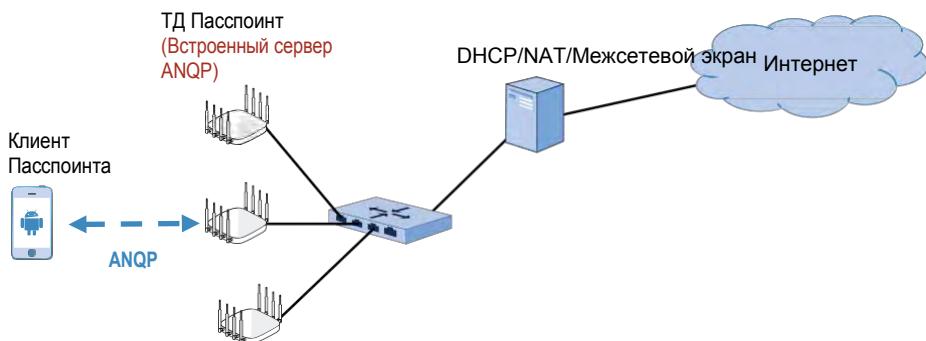
Еще одна растущая тенденция с сетями с публичным доступом – это использование 802.1X/EAP с технологией *Хотспот 2.0* [*Hotspot 2.0*]. Хотспот 2.0 это техническая спецификация Wi-Fi Альянса, которая поддерживается сертификационной программой Пасспоинт [Passpoint certification program]. С Хотспот 2.0 клиентские устройства БЛВС оснащаются сотовым оператором связи одним или более учетными данными, такими как SIM карта, парой имя пользователя/пароль, или сертификатом X.509. Многое из технической спецификации Хотспот 2.0 основано на механизмах, изначально определенных поправкой IEEE 802.11u-2011. Две основные цели технической спецификации Хотспот 2.0:

- Сделать публичные/комерческие Wi-Fi сети такими же безопасными и простыми в использовании, как и корпоративные/домашние Wi-Fi сети
- Направить (сгрузить) сотовый 3G/4G сетевой трафик в Wi-Fi сети

*Пасспоинт* [Passpoint] – это бренд для сертификационной программы, управляемой Wi-Fi Альянсом. Сертификация Пасспоинт [Passpoint] основана на спецификации Хотспот 2.0 Wi-Fi Альянса. Устройства, которые прошли эти сертификационные испытания могут называться «Устройства Пасспоинт» [“Passpoint devices.”]

## Протокол Опроса Сетей Доступа

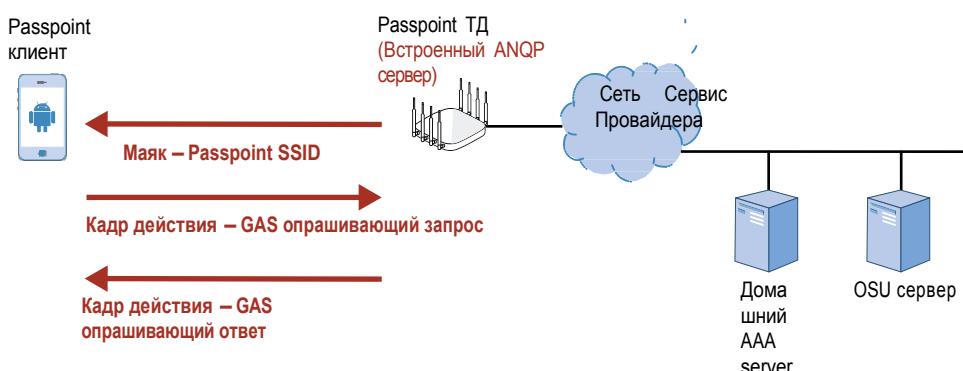
Устройства Пасспоинт [Passpoint devices] могут опрашивать БЛВС, прежде чем подключиться, для того, чтобы обнаружить сотовых операторов, поддерживаемых сетью. Устройства Пасспоинт[Passpoint] используют *Протокол Опроса Сетей Доступа* [Access Network Query Protocol (ANQP)], протокол вопросов и ответов, определенный 802.11u. Как показано на Рисунке 18.28, необходим сервер ANQP, чтобы отвечать на ANQP опросы от клиентов Пасспоинта [Passpoint]. Сервер ANQP может быть отдельным сервером или встроенным в точки доступа.

**РИСУНОК 18.28 ANQP**

ANQP используется мобильными устройствами с поддержкой Пасспоинт [Passpoint], чтобы обнаружить целый диапазон информации, включая следующее:

- Наименование места [Venue name]
- Требуемые типы аутентификации, такие как EAP-AKA или EAP-TLS
- Информация о сотовых сетях 3GPP, доступных через точку доступа.
- Роуминговый консорциум (для хотспотов с роуминговыми соглашениями с другими сервис провайдерами)
- Идентификатор Сетевого Адреса (NAI) дома [Network Address Identifier (NAI) home]
- Диапазоны идентификаторов сетевых адресов (NAI), доступных через ТД [NAI realms accessible through the AP]
- Параметры WAN
- Многое другое

Информации ANQP в кадре Маяка обычно не достаточно для того, чтобы Пасспоинт клиент [Passpoint client] подключился к Passpoint SSID. Следовательно, Пасспоинт клиент использует кадры опроса Универсального Сервиса Оповещений [Generic Advertisement Service (GAS)], чтобы собрать большую часть необходимой информации от сервера ANQP, как показано на Рисунке 18.29.

**РИСУНОК 18.29 GAS опросы**

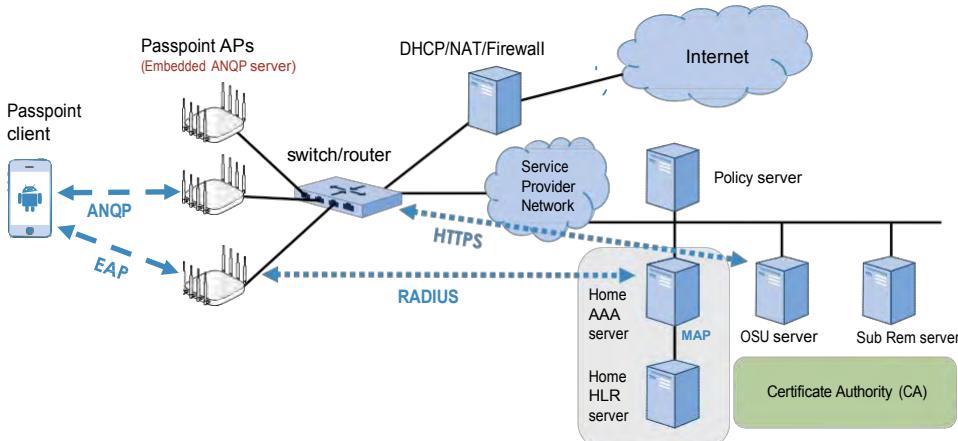
## Архитектура Хотспот 2.0

Сложность технической спецификации Хотспот 2.0 – это интеграция со всеми тыльными [backend] серверами сети сотового сервис провайдера, как показано на Рисунке 18.30.

Компоненты сервиса провайдера включают следующее:

- Сервер Онлайн Регистрации [Online Sign Up (OSU)] используется для создания новой учетной записи для нового пользователя/устройства во время регистрации. HTTPS используется между мобильным устройством и сервером OSU для регистрации и обеспечения нового абонента [subscriber] Хотспота.
- Сервер Восстановления Подписки [Subscription Remediation (Sub Rem)] используется для восстановления информации о подписке для пользователя после регистрации. Например: закончился срок действия пароля или есть неоплаченный платеж.
- Сервер Политики [Policy server] используется для передачи на мобильное устройство сетевой политикой после регистрации.
- EAP и RADIUS используется для подтверждения учетных данных клиента Passpoint у сервера AAA Домашнего оператора. Клиенты Passpoint используют протокол 802.1X/EAP, и кадры EAP пересыпаются на Домашний AAA сервер в RADIUS пакетах.
- Сервер Реестра в Домашней Локации [Home Location Register (HLR)] - это локальный сервер регистрации для сотовых сетей 3G/4G.
- Домашний AAA сервер взаимодействует с сервером HLR касательно устройств с SIM или USIM карт.
- Подсистема Мобильных Приложений [Mobile Application Part (MAP)]- это протокол телефонной системы сигнализации для Реестра в Домашней Локации [Home Location Register (HLR)].
- Центр Сертификации(ЦС) [Certificate Authority (CA)] выпускает сертификаты для AAA сервера, OSU сервера, Sub Rem сервера, и сервера Политик [Policy].
- Если необходимо, Центр Сертификации (CA) также используется для оснащения клиентов Passpoint сертификатами.

**РИСУНОК 18.30** БЛВС Хотспот 2.0



## 802.1X/EAP и Хотспот 2.0

Поскольку Хотспот 2.0 требует безопасность 802.1X/EAP, все устройства имеют уникальный аутентификационный идентификатор, и трафик шифруется на SSID Пасспоинта. Таблица 18.1 перечисляет поддерживаемые учетные данные и методы EAP Для БЛВС Хотспот 2.0.

**ТАБЛИЦА 18.1** Хотспот 2.0—поддерживаемые клиентские учетные данные и EAP протоколы

| Тип Учетных Данных       | Метод EAP |
|--------------------------|-----------|
| Клиентский сертификат    | EAP-TLS   |
| SIM карта                | EAP-SIM   |
| USIM карта               | EAP-AKA   |
| Имя пользователя /пароль | EAP-TTLS  |

*EAP- Модуль Идентификации Абонента [EAP-Subscriber Identity Module (EAP-SIM)]* в первую очередь был разработан для отрасли мобильных телефонов и более конкретно для второго поколения (2G) мобильных сетей. Многие из нас, у кого есть мобильные телефоны, знакомы с концепцией карты *Модуля Идентификации Абонента [Subscriber Identity Module (SIM)]*-т.е. SIM-карты. SIM карта - это устройство встроенной идентификации и хранения, очень похожее на смарт карту. SIM карты маленькие и вставляются в небольшие мобильные устройства, как сотовые или мобильные телефоны в отношении 1:1 к устройству в любое время. Глобальная Система для Мобильной Связи [Global System for Mobile Communications (GSM)] является стандартом мобильных сетей второго поколения. EAP-SIM, описанные в IETF RFC 4186, специфицируют механизмы EAP, которые основаны на аутентификации мобильных сетей GSM 2G и примитивах соглашений о ключах. Для операторов мобильных телефонов это значимая часть информации, которая может быть использована для аутентификации. EAP-SIM не предлагает взаимной аутентификации, и длины ключей намного короче, чем механизмы, используемые в мобильных сетях третьего поколения (3G).

*EAP-Аутентификация и Соглашение о Ключах [EAP-Authentication and Key Agreement (EAP-AKA)]* - это тип EAP, в первую очередь разработанный для отрасли мобильных телефонов и, в частности, для 3G мобильных сетей. EAP-AKA, описанный в IETF RFC 4187, определяет использование аутентификации и механизмов соглашения о ключах уже используется двумя типами 3G мобильных сетей. Мобильные сети 3G включают в себя Универсальную Мобильную Телекоммуникационную Систему [Universal Mobile Telecommunications System (UTMS)] и CDMA2000. AKA обычно работает в SIM модуле. SIM модуль может также называться как *Универсальный Модуль Идентификации Абонента [Universal Subscriber Identity Module (USIM)]* или *Убираемый Модуль Идентификации Пользователя [Removable User Identity Module (R-UIM)]*. AKA основан на механизмах вызов-ответ [challenge-response] и симметричной криптографии, и работает в модулях USIM или R-UIM. Длины ключей шифрования могут быть существенно длиннее, и теперь может быть использована взаимная аутентификация. EAP-AKA может также быть использована в мобильных сетях 4G, которые обычно используют сотовую технологию *Долгосрочной Эволюции [Long Term Evolution (LTE)]*. Еще один протокол, называемый *5G-AKA* также был определен для сотовых сетей 5G.

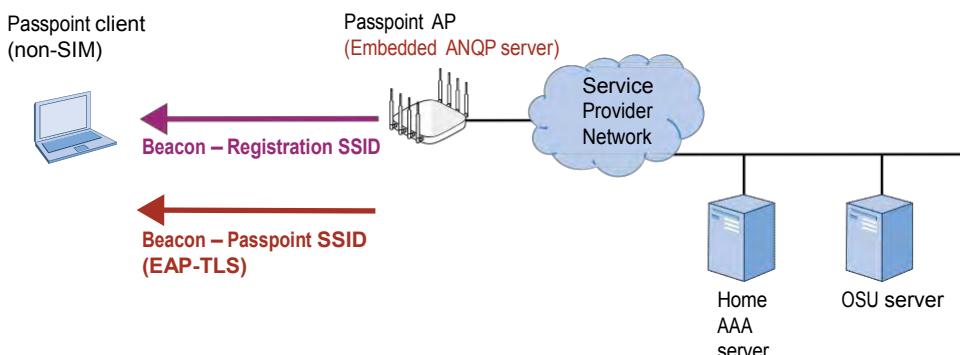
Пасспоинт устройства без SIM карты [Non-SIM Passpoint devices], такие как ноутбуки, используют безопасность или EAP-TLS или EAP-TTLS.

*EAP Безопасность Транспортного Уровня [EAP Transport Layer Security (EAP-TLS)]* определена в IETF RFC 5216 и является широко используемым протоколом безопасности. EAP-TLS считается одним из наиболее безопасных EAP методов, используемых в БЛВС на сегодня. EAP-TLS требует использование сертификатов с клиентской стороны в дополнение к сертификатам с серверной стороны. Сертификаты клиентской стороны используются в качестве учетных данных для клиентского устройства. *EAP - Туннелированной Безопасности Транспортного Уровня [EAP-Tunneled Transport Layer Security (EAP-TTLS)]* требует только использование серверных сертификатов, и определена в IETF RFC 5281. В EAP-TTLS, учетные данные типа: имя пользователя и пароль безопасно аутентифицируются в SSL туннеле. Как для большинства методов EAP, требуется безопасная доставка корневых сертификатов, и возможно клиентских сертификатов. Безопасная доставка сертификатов происходит во время процесса онлайн регистрации [*online sign-up (OSU)*] в любой БЛВС Хотспот 2.0.

## Онлайн Регистрация

Существует два варианта онлайн регистрации [*online sign-up (OSU)*], которые клиенты с поддержкой Passpoint используют для первоначальной регистрации, и затем подключаются к безопасному SSID Пасспоинта. Как показано на Рисунке 18.31, оба метода требуют двух SSID— один SSID для первоначальной регистрации, а второй безопасный SSID Пасспоинта.

**РИСУНОК 18.31** Онлайн регистрация



Первый вариант позволяет операторам хотспотов использовать устаревший открытый SSID, который не использует шифрование. Клиент Пасспоинта сначала подключается к открытому SSID, чтобы зарегистрироваться у сервис провайдера. Затем клиент перенаправляется на перехватывающий веб портал [*captive web portal*], который защищен с помощью HTTPS. На перехватывающем веб портале клиент выбирает сервис провайдера и продолжает процесс регистрации. Регистрация между клиентским устройством и OSU сервером защищена HTTPS. Во время процесса регистрации сертификаты EAP-TLS и клиентские учетные данные, предоставляемые сервис провайдером, могут быть переданы и установлены на клиентское устройство. По завершении регистрации клиент отключается от регистрационного SSID [*sign-up SSID*] и затем подключается к защищенному SSID Пасспоинта с помощью 802.1X/EAP.

Второй вариант онлайн регистрации также использует два SSID; однако, первичный регистрационный SSID, называется как SSID *Шифрованная L2Сеть с Аутентификацией только на Серверах с Онлайн Регистрацией* [*OSU Server-Only Authenticated L2 Encryption*

*Network (OSEN)*]. Также как в первом варианте, регистрация между клиентским устройством и OSU сервером защищена HTTPS. Основная разница в том, что SSID регистрации OSEN подразумевает защиту связи других мобильных устройств, не связанных с клиентской регистрацией. OSEN SSID использует *Анонимный EAP-TLS* [*Anonymous EAP-TLS*], который аутентифицирует только сеть сервис провайдера, а не клиента. Цель в гарантировании, что сеть сервис провайдера легитимна.

Во время процесса регистрации, сертификаты и клиентские учетные данные предоставленные сервис провайдером могут быть переданы и установлены на клиентском устройстве. По завершении регистрации, клиентское устройство отключается от OSEN SSID и затем должно подключиться к безопасной SSID Пасспоинта с использованием 802.1X/EAP. Если OSEN SSIDs используются клиентами Пасспоинта для регистрации, третий открытый SSID вероятнее всего будет присутствовать для подключения к БЛВС для устаревших не-Пасспоинт [non-Passpoint] клиентов.

## Роуминговые Соглашения

У сотовых сервис провайдеров также могут быть соглашения о роуминге с другими сервис провайдерами. Не перепутайте это с механизмами роуминга 802.11, которые обсуждались ранее в этой книге. Роуминговое соглашение сервис провайдеров - это просто деловое взаимодействие между разными сервис провайдерами. Заказчики одного провайдера хотспотов могут подключаться к сервисам БЛВС хотспотов другого сотового провайдера без дополнительной платы. Информация о применимом роуминговом соглашении предоставляется клиентам Пасспоинта по протоколу ANQP. Пасспоинт допускает межоператорский роуминг, с обнаружением, аутентификацией и учетом. Технология Хотспот 2.0 и Пасспоинт изначально предназначались для сетей сотовых операторов; однако, существуют некоторые возможности для использования ANQP для БЛВС гостевого доступа в частных корпоративных сетях.

Цель Хотспота 2.0 - обеспечить безопасную аутентификацию и шифрование БЛВС публичного доступа. Хотя открытые сети все еще являются нормой сегодня, растущий интерес в безопасности и автоматического подключения в сетях публичного доступа могут мотивировать более широкое принятие и использование технологии Хотспот 2.0. Многие из основных аэропортов в Соединенных Штатах теперь поддерживают Хотспот 2.0. Интуитивная программа Европейской Комиссии WiFi4EU способствует бесплатному подключению к Wi-Fi граждан и посетителей на общественных пространствах таких как парки, площади, общественные здания, библиотеки и музеи по всей Европе. WiFi4EU. требует Хотспот 2.0 и Пасспоинт. Вы можете узнать больше о WiFi4EU по адресу <https://wifi4eu.ec.europa.eu>.

Держите в уме, что клиенты и точки доступа должны быть Пасспоинт сертифицированными [Passpoint-certified] и использовать Протокол Опроса Сетей Доступа [Access Network Query Protocol (ANQP)]. На текущий момент существует свыше 2800 уникальных Wi-Fi СЕРТИФИЦИРОВАННЫХ Пасспоинт [Wi-Fi CERTIFIED Passpoint] устройств. Дополнительно, существует родная поддержка в операционных системах Android, iOS, macOS, и Windows 10.

Устаревшие устройства БЛВС не поддерживают ANQP и не могут использовать преимущества технологии Хотспот 2.0, хотя последние версии большинства операционных систем поддерживают ранние версии Пасспоинт. Как вы, надеюсь, уже догадались, тыльная [backend] интеграция с сетями сервис провайдеров чрезвычайно сложная. Из-за этой сложности, принятие технологии очень медленное, и многие операторы до сих пор не используют эту технологию. Появление будущей сотовой технологии 5G также может иметь последствия для будущих внедрений.

## Контроль Сетевого Доступа

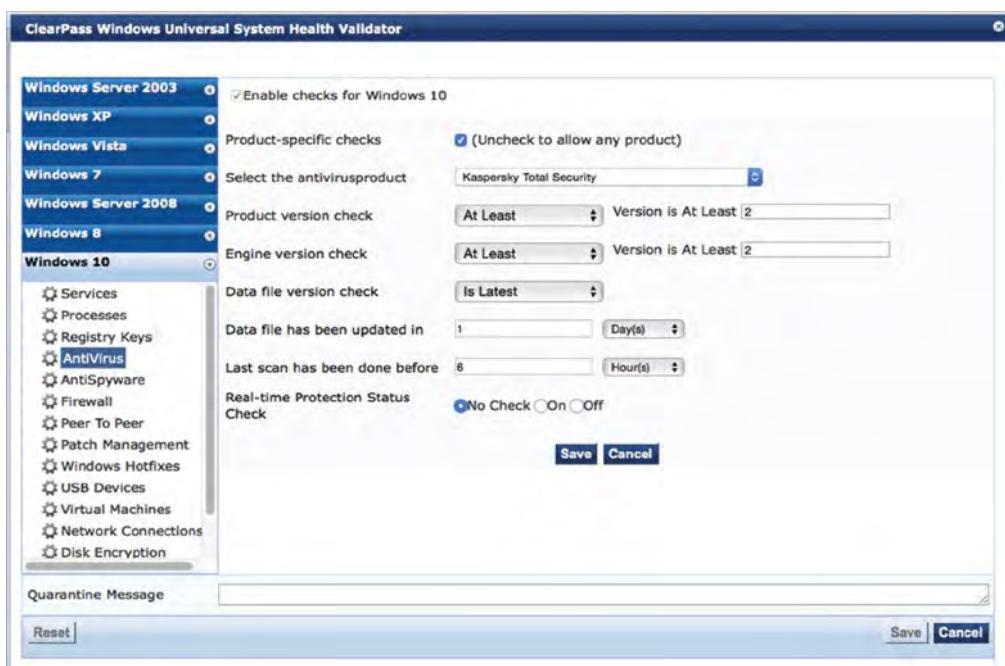
*Контроль сетевого доступа [Network access control (NAC)]* оценивает возможности или состояние компьютера, чтобы определить потенциальный риск компьютера для сети, и чтобы определить какой уровень доступа разрешить. NAC изменился с годами из среды, которая в первую очередь оценивала риск от вирусов и шпионского программного обеспечения

886 Глава 18 • Приноси Свое Собственное Устройство (BYOD) и Гостевой Доступ до среды, где на компьютере проводятся проверки и отпечатки, тщательно проверяя его возможности и настройки. Эти проверки интегрированы в 802.1X/EAP и RADIUS для аутентификации и авторизации сети доступа для пользователя и компьютера. При обсуждении NAC, беспроводные клиентские устройства часто называются конечными точками [endpoints].

## Состояние

NAC возник как ответ на компьютерные вирусы, черви и вредоносное ПО, которое появилось в начале 2000х. Ранние продукты NAC относятся примерно к 2003 году и предоставляли, что называется *оценку состояния* [posture assessment]. Оценка состояния - это процесс, который применяет набор правил проверки состояния и настройки компьютера, и определяет следует ли предоставить доступ к сети. Продукты NAC не производят проверку состояния самостоятельно, а скорее подтверждают, что соблюдается политика. Ключевая задача оценки состояния - убедиться, что программное обеспечение по безопасности (антивирус [antivirus], антишпионское ПО [antispyware], и межсетевой экран [firewall]) установлено, обновлено, и работает. Рисунок 18.32 показывает пример некоторых настроек антивируса, которые могут быть проверены. Фактически, оценка состояния [posture assessment] “проверяет проверяющих”. В дополнение к проверке программного обеспечения безопасности, оценка состояния может проверить состояние операционной системы. Политика состояния [Posture policy] может быть настроена так, чтобы гарантировать, чтобы определенные заплатки (патчи) или обновления были установлены, подтвердить, что определенные процессы запущены или не запущены, или даже проверить активно ли или нет определенное оборудование (например USB порты).

РИСУНОК 18.32 Настройки состояния Антивируса



Проверка состояния выполняется *постоянным агентом* [*persistent agent*] (программное обеспечение, которое постоянно установлено на компьютере) или *временным агентом* [*dissolvable agent*] (программа, которая устанавливается временно). Если компания развертывает установку программы проверки состояния, то вероятно будет установлен постоянный агент на всех корпоративных ноутбуках, чтобы гарантировать, что все они в хорошем состоянии. Компания также может захотеть проверять гостевые компьютеры, которые пытаются подключиться к сети; однако, гость вряд ли разрешить вашей компании установить программу на его компьютер. Когда гость подключается к перехватывающему порталу [*captive portal*], процесс оценки состояния может быть временно запущен, а гостевой компьютер проверен на соответствие.

После проведения проверки состояния, если компьютер считается нездоровым, то в идеальном сценарии агент проверки состояния автоматически вылечит или исправит проблемы, так чтобы компьютер смог пройти проверку и получить доступ к сети. Так как на корпоративных компьютерах установлен постоянный агент, и он обычно имеет права на внесение изменений, то может быть проведено автоматическое исправление [*automatic remediation*]. Компьютеры, на которых работает временные агенты, обычно не могут быть автоматически обновлены. Гостевые пользователи должны решить проблемы самостоятельно прежде чем получать доступ к сети.

Опыт конечного пользователя является существенным аспектом успешной оценки состояния. Если компьютер обнаружил, что не соответствует политике, то возможно несколько действий. Администратор может выбрать только сигнал тревоги по этой проблеме на панели мониторинга NAC, без какого либо взаимодействия с пользователем. Другой вариант - оповестить конечного пользователя о проблеме через сообщение в веб браузере или электронной почты, предоставляя ему инструкции по решению проблемы и возможно сообщая предупреждения и требования для решения. Далее, администратор может предпочесть поместить компьютер в карантин, пока проблемы не будут решены.

Обычно, карантинные точки доступа имеют доступ к сетевым ресурсам, требующимся для решения проблемы (например, установки клиента антивируса), но без другого доступа. В идеальном сценарии постоянному агенту будет разрешено автоматически исправить или вылечить проблемы так, чтобы компьютер смог пройти проверку и получить доступ к сети. Так как постоянный агент установлен на корпоративном компьютере и обычно имеет права на внесение изменений, то программа может автоматически все исправить.

Автоматическое исправление часто является сложным для настройки. Многие решения проверки состояний не включают эту возможность, полагаясь, вместо этого, на сообщение конечному пользователю, описывающее как решить проблему самостоятельно. Самостоятельное исправление часто является лучшим выбором.

## Отпечаток ОС

Наиболее точный взгляд на тип устройства и ОС бывает, когда установлен постоянный агент оценки состояния на конечной точке. Агент постоянной оценки состояния предлагает расширенный доступ к устройству, и, следовательно, может различить разные версии ОС и уровни патчей. В то время как это полезно для корпоративных устройств, таких как ноутбуки, агенты обычно не установлены на конечных устройствах BYOD или IoT устройствах. Однако, существует огромное разнообразие в IoT и BYOD устройствах, и, следовательно, есть реальная необходимость их видимости.

Адрес организационного уникального идентификатора [*organizationally unique identifier (OUI)*] - это первые три октета MAC адреса устройства, которые

**888** Глава 18 • Приноси Свое Собственное Устройство (BYOD) и Гостевой Доступ  
иdentифицируют производителя сетевого устройства. Оставшиеся октеты MAC адреса  
уникальны и используются для идентификации индивидуального устройства.  
IEEE присваивает OUI адреса производителям. Большинство решений используют  
соответствие OUI в качестве первого уровня уникального отпечатка [fingerprinting]  
устройства. Например, соответствие OUI - это простой метод про различению устройств,  
произведенных компанией Apple, от произведенных компанией Samsung.

*DHCP анализ [DHCP analysis]* использует DHCP рукопожатие, чтобы определить тип устройства, которое запрашивает сетевой адрес, следующее действие – это отправка DHCP запроса на получение IP адреса. Как часть этого запроса, клиентское устройство включает информацию DHCP и запрашивает список DHCP параметров или опций от DHCP сервера. Эти опции могут включать маску подсети, имя домена, шлюз по-умолчанию, и тому подобное. Когда клиент посыпает DHCP сообщения обнаружения [discover] и запроса [request], каждый тип клиентского запроса отличается параметрами в DHCP опции 55 части запроса. Параметры в DHCP опции 55 создают уникальный отпечаток [fingerprint], который может быть использован для идентификации операционной системы клиента.

Например, iOS устройства включают типовой набор параметров при выполнении DHCP запроса, таким образом делая возможным идентифицировать, что устройство скорее всего iOS устройство. Уникальный отпечаток DHCP не идеален, и часто невозможно понять различия между похожими устройствами, такими как iPod, iPhone, или iPad. В зависимости от производителя NAC, уникальный отпечаток DHCP [DHCP fingerprint] называется, как ASCII список опций параметров запроса, таких как 1, 3, 6, 15, 119, 252. Или то может быть представлено как шестнадцатеричная строка, например, 370103060F77FC. В строке две первые шестнадцатеричные цифры равны ASCII 55 (опция 55), а каждые следующие пары двух цифр являются шестнадцатеричными значениями каждой опции.

Вы можете найти расширенный список уникальный отпечатков DHCP на [www.fingerbank.org](http://www.fingerbank.org). Хотя список параметров запроса не гарантирует быть уникальным, он может обычно использоваться вместе с другими техниками уникальных отпечатков, чтобы идентифицировать устройства.

Еще один метод определения ОС – это уникальный HTTP отпечаток [*HTTP fingerprinting*]. Заголовок user-agent в HTTP пакете идентифицирует клиентскую операционную систему. Во время аутентификации на перехватывающем портале решения NAC способны проверить кадры HTTP/HTTPS при обработке клиентских запросов. Эта информация уникального отпечатка комбинируется с информацией, полученной через другие методы, чтобы лучше раскрасить клиентское устройство. Рисунок 18.33 показывает профиль устройства планшета Samsung Galaxy, использующего Android OS, идентифицируемую по OUI адресу, DHCP отпечатку, и HTTP user-agent отпечатку.

**РИСУНОК 18.33** Уникальный отпечаток ОС



Другой способ получения информации о клиентской ОС – это SNMP и TCP сканирование. Например, изначальное время жизни [time to live (TTL)] в IP заголовке и размер приемного TCP окна первого пакета в TCP сессии также могут быть использованы для идентификации некоторых операционных систем.

Когда администратор обладает точной информацией о типах устройств, используемых на сети, он может установить дифференцированный доступ на основе этих данных. Например, организация может захотеть позволить ноутбукам, планшетам и смартфонам быть в ее гостевой сети, и может выбрать запрет для игровых систем и других развлекательных устройств. Еще один типовой пример использования определяет список разрешенных операционных систем в ее корпоративной или безопасной SSID, чтобы защитить эту часть сети от неподтвержденных версий ОС или устройств.

IoT устройства, такие как сенсоры, могут быть размещены в отдельном VLANe с очень специфичными политиками доступа. Например, оборудование мониторинга пациента в больнице может подключаться к корпоративной SSID, но быть ограниченным определенным VLANом и иметь доступ только к необходимым мониторинговым серверам в сети больницы. Взрывной рост IoT устройств на рабочих местах сделал профилирование устройств очевидной необходимости.

## AAA

Ранее в книге мы упоминали аутентификацию, авторизацию и учет [authentication, authorization, and accounting (AAA)]. AAA это ключевые компоненты NAC. Аутентификация, очевидно, используется для идентификации пользователя, который подключается к сети. Мы часто называем это как определение “кто ты” [“who you are.”] Хотя “кто ты” – это очень важная часть процесса для разрешения доступа к сети, одинаково важный компонент подключения – авторизация. Мы часто называем это как определение “какая твоя роль” [“what you are.”] Авторизация используется для анализа информации такой как:

- Тип пользователя (администратор, поддержка, персонал) [User type (admin, help desk, staff)]
- Местоположение, тип подключения (беспроводное, проводное, VPN).
- Время дня
- Тип устройства (смартфон, планшет, компьютер)
- Операционная система
- Состояние (состояние системы) [Posture (system health or status)]

При настройке AAA для аутентификации, одна из задач – это определить или специфицировать базу данных, которая будет использоваться для подтверждения личности пользователя.

Исторически мы называем это как база данных пользователей [user database]; однако, личность пользователя может быть подтверждена чем-то другим, кроме учетной записи пользователя и пароля, например, MAC адресом или сертификатом. Если вы не уверены в типе идентификации, которая используется, или если вы хотите придерживаться более нейтральной позиции, то термин идентификационное хранилище [*identity store*] – будет нормальным для использования.

Путем использования и аутентификации и авторизации NAC может различать между Джоффом, использующим свой смартфон, и Джоффом, использующим свой персональный ноутбук. Из этой информации NAC может контролировать что Джофф может делать с каждым устройством на сети.

Чтобы использовать аналогию для объяснения авторизации, скажем что Джордж является членом сельского клуба. Когда он въезжает на территорию, охрана на въезде проверяет его идентификационную карту (пропуск) и подтверждает его членство.

Он был аутентифицирован. После того, как он припарковал свой автомобиль, он решает пойти в ресторан, так как сейчас 6:30 вечера и он голоден. Когда он приходит в ресторан, ему говорят, что ему не разрешено в ресторан. Смутившись, вопрос Джорджа – почему, так как он уже подтвердил, что он член клуба на входе. Хозяйка объясняет ему, что после 6.00 вечера у ресторана есть политика, что все гости мужчины должны быть одеты в слаксы (широкие мужские брюки) и пиджак. К сожалению, Джордж был одет в шорты и у него не было пиджака; следовательно, он не был авторизован (не прошел авторизацию) чтобы есть в ресторане. Хозяйка была учтивой и сказала Джорджу, что он авторизован (ему можно) пойти в холл и поесть там, так как требования для холла не такие строгие.

Как вы можете видеть из аналогии, аутентификация – это про то, кто вы, а авторизация – это про другие параметры, такие как что, где, когда и как. Также, в отличие от аутентификации, когда вы аутентифицированы или не аутентифицированы, авторизация варьируется от параметров и ситуации.

## Изменение Авторизации [CoA] по RADIUS

Системы NAC также могут автоматически и динамически определять сетевой доступ для выбранного устройства. Этот доступ может базироваться на первоначальной оценке при подключении к сети, или измениться впоследствии на основе изменения сетевого поведения или статус конечного устройства.

Изменение Авторизации по RADIUS [RADIUS *Change of Authorization (CoA)*] это функция, которая позволяет RADIUS серверу менять настройки активной клиентской сессии. CoA сообщения используются структурой AAA для динамического изменения сессий абонентов. Например, если изменяется состояние конечной точки, сообщение RADIUS CoA может обновить авторизационную политику конечной точки.

До RADIUS CoA, если клиенты аутентифицировались и им назначался набор разрешений на сети, то клиентская авторизация больше не менялась, пока клиент не выйдет [logged out] и не войдет снова [logged back in]. Это единственное разрешенное авторизационное решение делается при начальном установлении соединения клиентом.

Учет по RADIUS [accounting] (последняя *A* в AAA) используется для мониторинга пользовательского соединения. В ранние дни AAA, они обычно отслеживали активность клиентского соединения: события входа [logging in] и выхода [logging off], которые в некоторых средах могут быть всем тем, что вы хотите или вам нужно отслеживать.

Улучшения в учете [accounting] позволяют серверу AAA также предоставлять учет по времени [interim accounting]. Учет по времени может отследить ресурсную активность такую как время или байты, использованные для соединения. Если пользователь превысит или нарушит разрешенные лимиты ресурсов, то RADIUS CoA может быть использован для динамического изменения разрешений, которые есть у пользователя на сети. Изменения в поведении конечного устройства также могут запустить RADIUS CoA, и, следовательно, изменить сетевые права доступа. Например, NAC может перевести конечное устройство в изоляционную роль и изолированный VLAN, если обнаружено вредоносное ПО. Дополнительно, нарушение по полосе может стать результатом того, что конечное устройство и пользователь вернуться обратно к регистрационной роли.

Используя аналогию для объяснения RADIUS CoA, давайте скажем, что Джек собирается в клуб с друзьями попить коктейли и потанцевать. Когда они прибывают, вышибала в дверях пускает их в клуб, но говорит им, что им нельзя напиваться или создавать проблемы в клубе. Пока он это говорит им, вышибала убеждается, что они не пьяны и не вызывают проблем. К сожалению, вышибала должен стоять в дверях и мониторить гостей только при входе в клуб; вышибала не может мониторить гостей, когда они внутри клуба.

После нескольких ночей с некоторыми проблемами в клубе, управляющий решает нанять еще вышибал, которые будут проходить по клубу и следить за гостями, которые уже в клубе. Любой, кто обнаруживается пьяным или создающим проблемы или ограничивается в клубе (может быть больше не разрешено продавать алкогольные напитки), или удаляется из клуба. Когда такой гость находится за пределами клуба, то вышибала на входе может повторно оценить состояние гостя, возможно запретит повторный вход в клуб, возможно разрешит гостям вернуться в клуб, или разрешит гостям повторно войти с другим набором разрешений.

RADIUS CoA изначально был определен RFC 3576 и позже в RFC 5176. Прежде чем вы начали волноваться, нет, вам не нужно знать это для экзамена CWNA. Мы упомянули про это, потому что многие AAA серверы, NAC серверы, и корпоративное беспроводное оборудование ссылается на “RADIUS RFC 3576” в конфигурационном меню без отсылки к CoA. Следовательно, с практической точки зрения, вам следует знать, что если вы видите RFC 3576 в любом конфигурационном меню, то это раздел, где настраивается RADIUS CoA.

## Единый вход [Single Sign-On]

В ранние дни сетей передачи данных пользователи должны были входить [log in] на файловый сервер или сервер печати для того, чтобы получить доступ к сетевым ресурсам. Учетные записи пользователей управлялись и хранились на каждом сервере. Изначально, это редко было проблемой, поскольку сети были маленькие, но по мере роста числа внутренних серверов и типов серверов, входить [logging in] на несколько серверов стало напрягать. Чтобы упростить процесс, компании начали внедрять единый вход [*single sign-on (SSO)*] внутри организации, позволяя пользователям получить доступ к многим, если не ко всем внутренним ресурсам, используя единый сетевой вход [login]. Это не только упростило процесс входа [login] для пользователя, это также упростило управление сетью путем консолидации пользовательских учетных записей в одной центральной базе данных пользователей.

Внутри организации единый вход [*single sign-on*] хорошо работал много лет, пока корпоративные ресурсы не стали мигрировать на Интернет- и облачные- серверы и сервисы. Пользовательские логины [User logins] теперь должны были быть расширены за пределы корпоративной сети, а многие облачные серверы были действительно сервисами, предоставляемыми другими компаниями, такие как системы CRM, офисные приложения, базы знаний, и серверы обмена файлами. Аутентификация и авторизация, пересекающая организационные границы, добавила больше сложности и существенно больший риск безопасности.

Две технологии, Язык Разметки Утверждений Безопасности [*Security Assertion Markup Language (SAML)*] и OAuth, могут быть использованы для обеспечения безопасного доступа, необходимого для выхода за пределы сети организации. Следующие разделы кратко объясняют компоненты этих технологий и как они работают.

### SAML

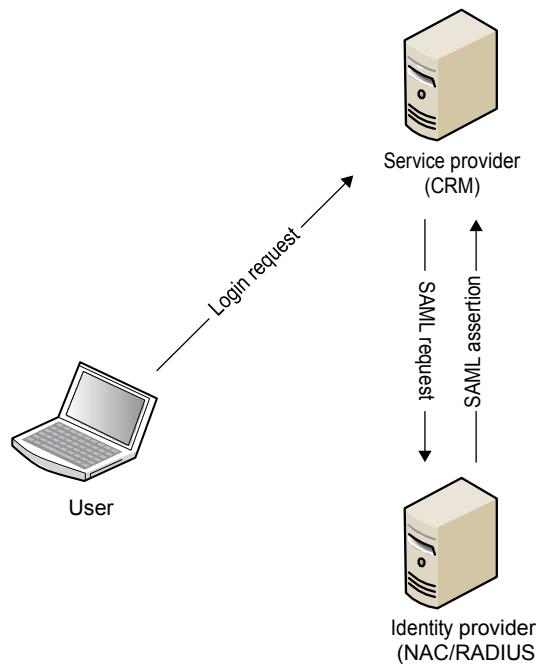
SAML предоставляет безопасный метод обмена пользовательской информацией о безопасности между вашей организацией и внешним сервис провайдером, таким как сторонняя облачная платформа управления взаимоотношениями с заказчиками [*customer relationship management (CRM)*]]. Когда пользователь пытается подключиться к платформе CRM, вместо требования к пользователю войти [log in], доверенная связь между вашим сервером аутентификации и сервером CRM подтверждает личность

пользователя и предоставляет доступ к приложению или сервису. Это позволяет пользователю входить [log in] разово в корпоративную сеть и затем незаметно и безопасно получать доступ к внешним сервисам и ресурсам без необходимости повторной проверки своей личности.

Спецификация SAML определяет три роли, которые участвуют в процессе SSO: поставщик идентификационной информации [identity provider (IdP)], который является подтверждающей стороной; сервис провайдер [service provider (SP)], который является доверяющей стороной [relying party]; и пользователь. Этот раздел кратко объясняет два сценария в которых SAML может быть использован для обеспечения SSO.

Первый сценарий - это сервис провайдер–инициировавший вход [login], как проиллюстрировано на Рисунке 18.34. Здесь, пользователь пытается получить доступ к ресурсам сервера CRM (SP). В этом сценарии, если пользователь не был аутентифицирован, то пользователь перенаправляется на корпоративный сервер аутентификации (IdP) с помощью запроса SAML. После успешной аутентификации, пользователь затем перенаправляется на сервер CRM с помощью утверждения SAML [SAML assertion], в этот раз пользователь получит доступ к запрошенным ресурсам.

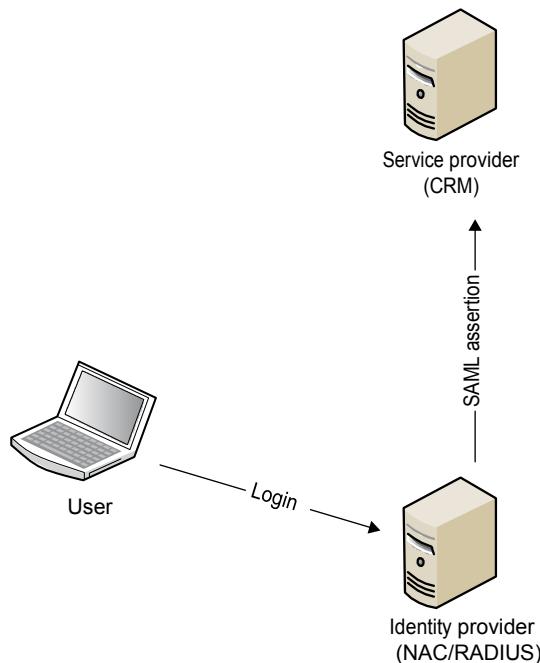
**РИСУНОК 18.34** Сервис провайдер–инициировал вход [login]



Второй сценарий - это провайдер идентификационной информации–инициировал вход [login], как проиллюстрировано на Рисунке 18.35. Здесь, пользователь входит [logs in] сначала на корпоративный сервер аутентификации (IdP). Зайдя, пользователь перенаправляется на сервер CRM и утверждение SAML [SAML assertion] подтверждает пользовательский доступ.

Существует много способов настройки SAML. Ключевая концепция в том, что он предоставляет доступ к ресурсам за пределами корпоративной сети, используя корпоративные учетные данные пользователя и не требуя от пользователя входить [log in] много раз.

РИСУНОК 18.3.5 Провайдер индентификационной информации–инициировал вход [login]



## OAuth

OAuth отличается от SAML; это авторизационный стандарт, а не аутентификационный стандарт. С OAuth пользователь входит [logs in] в аутентифицирующее приложение. После входа пользователь (владелец ресурса) может авторизовать стороннее приложение для доступа к определенной пользовательской информации или ресурсам, обеспечивая авторизационный поток для веб или обычных приложений, а также мобильных устройств. NACs могут использовать OAuth для связи с внешними ресурсами и системами.

## Итого

В этой главе мы обсуждали политики BYOD и решения MDM, которые нужны для управления мобильными устройствами компаний, а также мобильными устройствами сотрудников. Мы рассмотрели различия между устройствами компании и персональными устройствами, и подходы MDM политики для обоих. Мы обсудили различные компоненты архитектуры MDM и как компоненты взаимодействуют. Мы объяснили процесс регистрации MDM и процесс оснащения устройств настройками через эфир [over-the-air provisioning]. Мы рассмотрели типы мобильных устройств, которые используют программного MDM агента. Мы также обсудили управление через эфир [over-the-air] и управление приложениями, при использовании решения MDM для мобильных устройств.

Мы обсудили решения по самостоятельной регистрации устройств для сотрудников. Самостоятельная регистрация для устройств сотрудников самая быстро растущая тенденция для обеспечения BYOD.

Мы рассмотрели доступ к гостевым БЛВС и ключевые компоненты безопасности, необходимые для защиты корпоративной сетевой инфраструктуры от гостевых пользователей. Мы рассмотрели различные методы управления гостями, включая поручительство сотрудников, самостоятельная регистрация и логин социальных сетей. Мы также обсудили техническую спецификацию Хотспот 2.0 и сертификацию Wi-Fi Альянса Пасспоинт [Passpoint]. Наконец, мы обсудили как NAC может быть использован для обеспечения контроля доступа путем мониторинга состояния устройства и уникального отпечатка клиентского устройства прежде, чем оно подключится к сети. Сервисы AAA могут аутентифицировать пользователей, подключающихся к сети, и могут авторизовать устройство в сети. RADIUS CoA может быть использовано для модификации авторизации пользователя, если нужно назначить новый набор разрешений.

Хотя MDM, самостоятельная регистрация устройств, управление гостями, и NAC отдельные компоненты контроля сетевого доступа, мы решили написать обо всех четырех вместе в той главе, потому что несколько производителей БЛВС упаковывают эти решения безопасности вместе как один набор приложений. MDM, регистрация устройств, управление гостями БЛВС, и NAC могут быть развернуты как отдельные компоненты или в унисон, чтобы обеспечить управление безопасностью мобильных устройств, безопасностью гостевых пользователей, и безопасностью сетевого доступа.

## Темы Экзамена

**Определить различия между мобильными устройствами компании и персональными мобильными устройствами.** Уметь объяснить вопросы политики MDM для устройств компании и персональных мобильных устройств.

**Описать четыре главные компоненты архитектуры MDM.** Определить роли мобильного устройства, сервера MDM, ТД и сервера push уведомлений. Объяснить, как они взаимодействуют.

**Объяснить как MDM профили и MDM агенты используются в решении MDM.** Описать как MDM профили могут быть использованы для ограничений и настройки мобильных устройств. Описать роль агентов MDM и какие мобильные устройства требуют программного MDM агента.

**Обсудить управление MDM через эфир [over-the-air] и управление приложениями через MDM.** Уметь объяснить, как серверы push уведомлений используются для управления мобильными устройствами через Интернет. Объяснить, как решение MDM может управлять приложениями мобильных устройств.

**Объяснить самостоятельное управление устройством.** Уметь обсудить метод с двумя SSID и с одним SSID, используемым для обеспечения устройств сотрудниками. Объяснить преимущества и различия между самостоятельным управлением устройством и MDM.

**Определить четыре главных цели безопасности гостевой БЛВС.** Обсудить важность гостевых SSID, гостевых VLAN, гостевых политик межсетевого экрана, и перехватывающих веб порталов.

**Объяснить многие компоненты и методы управления гостями БЛВС.** Уметь объяснить самостоятельную регистрацию, поручительство сотрудником, логин социальный сетей, и другие ингредиенты управления гостями.

**Понимать техническую спецификацию Хотспот 2.0.** Описать, как клиентское устройство, с сертификацией Пасспоинт, может безопасно подключиться к сетям с публичным доступом через 802.1X/EAP.

**Объяснить NAC и как он используется для контроля доступа к сети.** Описать как состояние устройства, атрибуты RADIUS, и DHCP отпечаток используются вместе с AAA для аутентификации и авторизации пользователя и устройства в сети. Описать как RADIUS CoA может быть использовано для модификации авторизации пользователя.

# Контрольные Вопросы

1. В гостевых политиках межсетевого экрана какие из следующих портов рекомендуется разрешить? (Выберите все, что применимо.)

  - A.** TCP 22
  - B.** UDP 53
  - C.** TCP 443
  - D.** TCP 110
  - E.** UDP 4500
2. В гостевых политиках межсетевого экрана, какие IP сети стоит ограничить? (Выберите все, что применимо.)

  - A.** 172.16.0.0/12
  - B.** 20.0.0.0/8
  - C.** 192.16.0.0/16
  - D.** 172.10.0.0/24
  - E.** 10.0.0.0/8
3. Что является компонентами в архитектуре MDM? (Выберите все, что применимо.)

  - A.** ТД
  - B.** RADIUS
  - C.** BYOD
  - D.** APNs
  - E.** GCM
4. Какие из методов, которые могут быть использованы для передачи корневого сертификата Wi-Fi клиентам, которые работают как клиенты 802.1X/EAP? (Выберите все, что применимо.)

  - A.** GPO
  - B.** RADIUS
  - C.** MDM
  - D.** APNs
  - E.** GCM
5. Какой протокол используется клиентским БЛВС устройством с сертификацией Пасспоинт [Passpoint] для обнаружения сотового сервис провайдера, поддерживаемого БЛВС Хотспот 2.0?

  - A.** DNS
  - B.** SCEP
  - C.** OAuth
  - D.** ANQP
  - E.** IGMP

- 6.** Какой тип информации может быть виден на мобильном устройстве, который мониторится сервером MDM? (Выберите все, что применимо.)
- A.** SMS сообщения
  - B.** Время жизни аккумуляторной батареи
  - C.** Историю веб просмотров
  - D.** Установленные приложения
  - E.** Емкость устройства
- 7.** Какие методы EAP могут быть использованы для аутентификации для клиента Пасспоинт для подключения к безопасному SSID Пасспоинта? (Выберите все, что применимо.)
- A.** EAP-PEAP
  - B.** EAP-TLS
  - C.** Анонимный EAP-TLS
  - D.** EAP-AKA
  - E.** EAP-LEAP
- 8.** Какие из методов, которые могут быть использованы перехватывающим порталом для перенаправления пользователя на страницу входа перехватывающего портала? (Выберите все, что применимо.)
- A.** Перенаправление HTTP
  - B.** Перенаправление IP
  - C.** Перенаправление UDP
  - D.** Перенаправление TCP
  - E.** Перенаправление DNS
- 9.** Во время процесса регистрации MDM, какие ресурсы могут быть доступны мобильному клиенту пока оно в карантине в огороженном саду [walled garden]? (Выберите все, что применимо.)
- A.** SMTP сервер
  - B.** DHCP сервер
  - C.** DNS сервер
  - D.** MDM сервер
  - E.** Exchange сервер
- 10.** Какой протокол используется устройствами iOS и macOS для передачи MDM профилей через эфир [over-the-air], использующий сертификаты и SSL шифрование?
- A.** OAuth
  - B.** GRE
  - C.** SCEP
  - D.** XML
  - E.** HTTPS

- 11.** Какой механизм может быть использован, если гостевой VLAN не поддерживается на границе сети и находится только в DMZ?
- A.** GRE
  - B.** VPN
  - C.** STP
  - D.** RTSP
  - E.** IGMP
- 12.** Какой тип решения управления гостями нужно интегрировать с LDAP?
- A.** Логин социальных сетей [Social login]
  - B.** Режим киоска
  - C.** Регистрация секретарем
  - D.** Самостоятельная регистрация
  - E.** Поручительство сотрудником
- 13.** Сотрудник зарегистрировал персональное устройство на MDM сервере через корпоративную БЛВС. Дома сотрудник удалил MDM профиль. Что произойдет с персональным устройством сотрудника в следующий раз, когда сотрудник попытается подключиться к SSID компании?
- A.** MDM сервер повторно передаст MDM профиль через эфир.
  - B.** Сервис push уведомлений повторно передаст MDM профиль через эфир.
  - C.** Устройство будет помещено в карантин в огороженный сад [walled garden] и будет повторно зарегистрировано [re-enroll].
  - D.** Устройство будет иметь свободный доступ ко всем ресурсам, потому что сертификат находится все еще на мобильном устройстве.
- 14.** Какая фраза лучше всего описывает политику разрешения сотрудникам подключаться собственными персональными устройствами, такими как смартфоны, планшеты, и ноутбуки к сети на рабочем месте?
- A.** MDM
  - B.** NAC
  - C.** DMZ
  - D.** BYOD
- 15.** Какой метод управления гостями может компания лучше всего использовать для сбора ценной персональной информации о гостевых пользователях?
- A.** Логин социальных сетей [Social login]
  - B.** Режим киоска
  - C.** Регистрация секретарем
  - D.** Самостоятельная регистрация
  - E.** Поручительство сотрудника

- 16.** Какой вид удаленных действий может администратор MDM отправить на мобильное устройство через Интернет?
- A.** Изменение настроек
  - B.** Изменение ограничений
  - C.** Блокировка устройства
  - D.** Очистка устройства
  - E.** Изменение приложений
  - F.** Все выше перечисленное
- 17.** Какие дополнительные ограничения могут быть наложены на гостевого пользователя, помимо тех, которые определены гостевой политикой межсетевого экрана? (Выберите все, что применимо.)
- A.** Шифрование
  - B.** Фильтрация содержимого веб
  - C.** DHCP snooping
  - D.** Ограничение скорости
  - E.** Изоляция клиентов
- 18.** В инфраструктуре БЛВС где может работать гостевой перехватывающий веб портал? (Выберите все, что применимо.)
- A.** ТД
  - B.** Контроллер БЛВС
  - C.** Сторонний сервер
  - D.** Облачный сервис
  - E.** Все выше перечисленное
- 19.** Когда развернутое решение MDM, после того как мобильное устройство подключилось к точке доступа, где мобильное устройство остается пока процесс регистрации MDM не завершен?
- A.** DMZ
  - B.** Огороженный сад [Walled garden]
  - C.** Карантинный VLAN [Quarantine VLAN]
  - D.** IT песочница [IT sandbox]
  - E.** Ничего из выше перечисленного
- 20.** Чтобы вычислить емкость, которую нужно иметь Джейффу на сети, что из следующего может сервер NAC использовать для начальной идентификации и установки разрешений? (Выберите все, что применимо.)
- A.** Оценка состояния [Posture assessment]
  - B.** Отпечаток DHCP [DHCP fingerprinting]
  - C.** Атрибуты RADIUS
  - D.** RADIUS CoA
  - E.** Логин социальных сетей [Social login]

# Глава 19



## 802.11ax: Высокая Эффективность

В ЭТОЙ ГЛАВЕ ВЫ УЗНАЕТЕ О СЛЕДУЮЩЕМ:

- ✓ 802.11ax = Wi-Fi 6
- ✓ Перегруженность Wi-Fi трафика
- ✓ Обзор Высокой Эффективности
- ✓ Много-пользовательский(MU)
  - Поднесущие
  - Ресурсные блоки
  - Триггерные кадры
  - OFDMA в нисходящем канале
  - OFDMA в восходящем канале
  - Отчеты состояния буфера
  - Индикация режима работы
- ✓ MU-MIMO
  - OBSS
  - Цвет BSS
  - Работа пространственного переиспользования
- ✓ Целевое время пробуждения
- ✓ Дополнительные возможности 802.11ax PHY и MAC
  - 1024-QAM
  - Длинное символьное время и защитные интервалы



- Заголовки PHY 802.11ax
- Только—20 МГц
- AMPDU с Множеством Идентификаторов Трафика (Multi-TID AMPDU)

#### ✓ Ключевые вопросы Wi-Fi 6

- Клиенты
- МультиГигабитный Ethernet
- Питание по Ethernet
- 4x4:4 или 8x8:8
- 80 МГц и 160 МГц каналы
- СЕРТИФИЦИРОВАННЫЙ Wi-Fi 6



С каждой новой еще черновой поправкой, IEEE предлагает улучшения к технологиям 802.11. В 2009 году принятие поправки 802.11n было огромной важности - изменение в способе работы Wi-Fi радиомодулей. 802.11n перешел от

радиомодулей один-вход, один-выход [single-input, single-output (SISO)] на радиомодули много-входов, много-выходов [multiple-input, multiple-output (MIMO)]. До технологии 802.11n радиоволновое явление многолучевого распространения[multipath] было деструктивным; однако, многолучевое распространение [multipath] действительно полезно для радиомодулей MIMO 802.11n/ac. Когда технология 802.11n вышла на рынок, инженеры БЛВС должны были заново узнавать, как работает технология 802.11 и переобдумывать проектирование БЛВС. В 2013 году 802.11ac представила дальнейшие улучшения, использующие радиомодули MIMO. Конечный результат 802.11n/ac был в более высоких скоростях передачи данных, но не в лучшей эффективности. Пока и 802.11n и 802.11ac улучшали производительность, технологии были более сложные, и, следовательно, появились новые вызовы проектирования БЛВС и решения проблем БЛВС.

Поправка IEEE 802.11ax определяет фундаментальные изменения в том, как взаимодействует Wi-Fi радиомодули. Черновик поправки 802.11ax называется технологией высокой эффективности [high efficiency (HE)], которая могла бы наиболее значительно изменить Wi-Fi с момента появления радиомодулей MIMO 802.11n в 2009 году. Пока это пишется, IEEE выпустил черновую версию 8.0 поправки 802.11ax, а финальная ратификация ожидается в Феврале 2021 года (как раз во время публикации этой книги).

802.11ax технология дебютировала на рынке с первым поколением чипсетов, появившихся в ТД, в конце 2018 года. К 2019 году все крупные производители БЛВС предлагали ТД 802.11ax, а клиентские радиомодули 802.11ax стали поставляться в смартфонах. Более того, Wi-Fi Альянс начал сертифицировать технологию 802.11ax в Августе 2019 года с новой сертификацией с названием СЕРТИФИЦИРОВАННЫЙ Wi-Fi 6 [Wi-Fi CERTIFIED 6]. Эта глава - верхнеуровневый обзор улучшений эффективности технологии 802.11ax.

## 802.11ax = Wi-Fi 6

*802.11ax* - это черновик поправки IEEE [на момент перевода это уже ратифицированная поправка], которая определяет изменения на Физическом уровне [Physical layer (PHY)] 802.11 и на подуровне Контроля Доступа к Среде [Medium Access Control (MAC)] 802.11 для работы высокой эффективности [high efficiency (HE)] в полосе частот между 1 ГГц и 6 ГГц. Точно также как очень *высокая пропускная способность [very high throughput (VHT)]* - это технический термин для 802.11ac, *высокая эффективность [high efficiency (HE)]* - это технический термин для 802.11ax.

Недавно, Wi-Fi Альянс принял новое соглашение о наименованиях поколений Wi-Fi технологий. Цель в том, чтобы новое соглашение о наименованиях было бы проще к пониманию для среднестатистического потребителя вместо набора букв в наименовании, используемых IEEE. Так как технология 802.11ax - это такой сдвиг парадигмы от предыдущих версий технологий 802.11, ему было присвоено название поколения - Wi-Fi 6.

Старые версии технологии 802.11 также выровняли в соответствии с новым соглашением о наименованиях. Например, 802.11ac может называться как Wi-Fi 5, а 802.11n как Wi-Fi 4, как показано на Рисунке 19.1.

**РИСУНОК 19.1** Поколения Wi-Fi



На протяжении этой главы мы будем использовать и терминологию IEEE 802.11 и терминологию поколений Wi-Fi Альянса. 802.11ax и Wi-Fi 6 подразумевают одну и ту же вещь, но термин Wi-Fi 6 будет более употребляемым в среде обычного населения. "Повернутые" профессионалы БЛВС могут использовать термин 802.11ax, хотя ваша бабушка скорее поймет наименование поколения Wi-Fi 6.

## Перегруженность Wi-Fi трафика

Хотя Wi-Fi это эластичная технология, она не обязательно была эффективной. Wi-Fi работает и на 1ом уровне, и на 2ом уровне модели OSI, а неэффективность присутствует на обоих уровнях.

Исторически, предыдущие поправки 802.11 определяли технологии, которые давали более высокие скорости передачи данных и более широкие каналы, но не решали вопросы с эффективностью. Наиболее часто приводимая аналогия - это то, что строится больше быстрых автомобилей и больше автомагистралей, а автомобильные пробки остаются. Несмотря на большие скорости передачи данных и 40/80/160 МГц каналы, используемые радиомодулями 802.11n/ac, множество факторов ведут к перегруженности Wi-Fi трафика, который не обеспечивает эффективного использования среды.

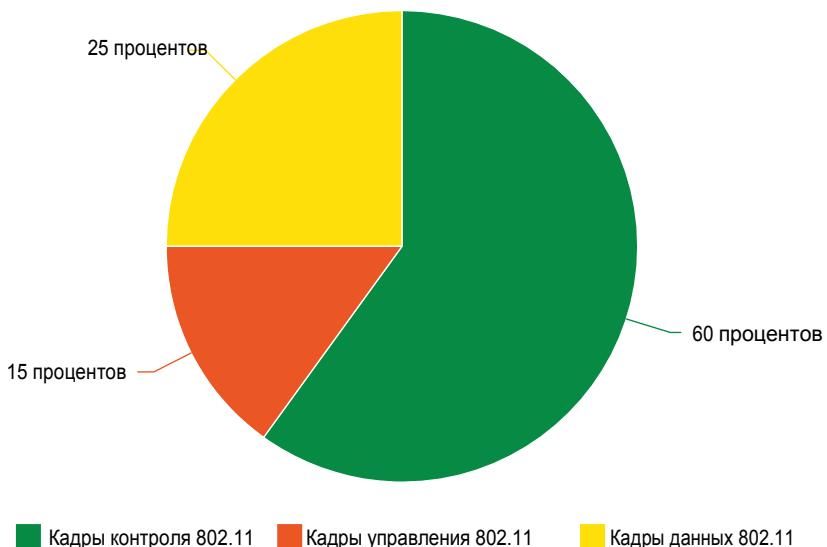
Годами основной акцент был на более быстрых скоростях и более высоких скоростях передачи данных для удовлетворения требований высокой плотности в корпоративных БЛВС. Однако, существует большая ошибочная концепция, что скорости передачи данных [data rates] это тоже самое, что и реальная пропускная способность [throughput]. И более того, скорость может быть переоценена. Чем хорош Феррари, который может ехать со скоростью 300 км в час, если Феррари застрял в пробке?

Итак, конкретно почему существует пробка в Wi-Fi трафике? Ранее вы узнали, что скорости передачи данных 802.11 это не пропускная способность TCP. Всегда помните, что радиоволновая среда - это полудуплексная среда, и что протокол борьбы за среду 802.11 CSMA/CA много потребляет из доступной полосы. В лабораторных условиях пропускная способность TCP в 60-70 процентов от рабочей скорости передачи данных может быть достигнута с использованием 802.11n/ac связи между одной точкой доступа (ТД) и одним клиентом. Числа агрегированной пропускной способности значительно меньше в средах реального мира с активным участием множества Wi-Fi клиентов, работающих через ТД. Чем больше клиентов борется за среду, тем значительнее растет количество служебной информации [overhead] при борьбе за среду и падает эффективность

Следовательно, агрегированная пропускная способность обычно составляет в лучшем случае 50 процентов от рекламируемой скорости передачи данных 802.11. Не очень эффективно.

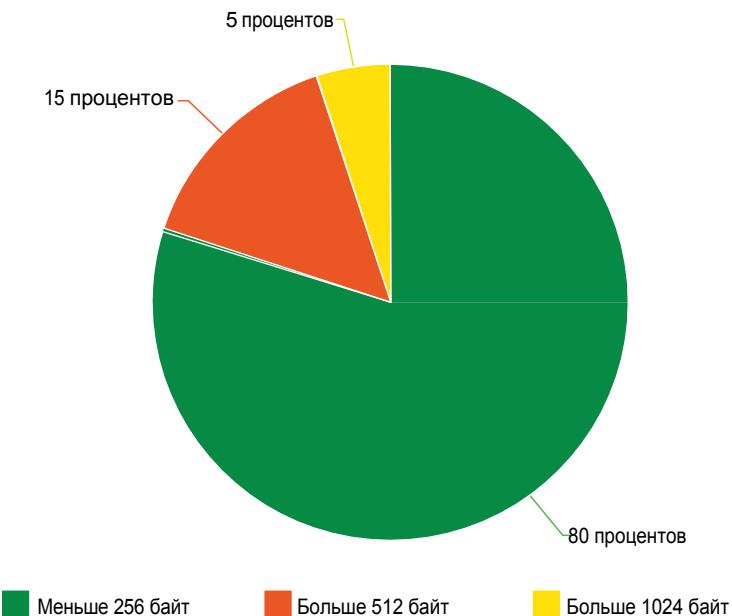
Что еще способствует перегруженности трафика 802.11? Так как устаревшие клиенты Wi-Fi часто присутствуют в корпоративных БЛВС, то необходим механизм защиты RTS/CTS, который способствует неэффективности. Как показано на Рисунке 19.2, около 60 процентов всего Wi-Fi трафика - это контрольные кадры 802.11, и 15 процентов - это кадры управления 802.11. Кадры контроля и управления занимают 75 процентов полезного эфирного времени [airtime], и только 25 процентов Wi-Fi трафика используется для кадров данных 802.11. Дополнительно, повторные передачи на 2ом уровне как результат радиоинтерференции или плохо спроектированной БЛВС может также способствовать неэффективности 802.11.

**РИСУНОК 19.2** Трафик 802.11



Высокие скорости передачи данных полезны для полезной нагрузки больших данных; однако основной объем кадров данных 802.11 (75-80 процентов) - это небольшие кадры меньше 256 байт, как показано на Рисунке 19.3. Каждый небольшой кадр требует заголовок PHY, MAC заголовок, и окончание. В результате имеем избыточную служебную информацию PHY/MAC и избыточные служебные накладные расходы борьбы за среду для каждого маленького кадра. Маленькие кадры могут быть агрегированы, чтобы уменьшить накладные расходы [overhead]; однако, в большинстве случаев, небольшие кадры не агрегируются, потому что они должны быть переданы последовательно из-за протоколов приложений верхних уровней. Например, пакеты VoIP не могут быть агрегированы, потому что они должны прибывать последовательно.

Несмотря на более высокие скорости передачи данных и широкие каналы, которые могут быть использованы радиомодулями 802.11n/ac, результат - перегруженный Wi-Fi трафик. Перегруженность автомобильного трафика может привести к тому, что водители становятся расстроеными и вовлекаются в агрессивное поведение на дороге. Технология Wi-Fi 6 (802.11ax) - это все про более лучшее управление трафиком [*traffic management*] 802.11 и, надеюсь, к устранению агрессивного Wi-Fi радиоповедения.

**РИСУНОК 19.3** Размер кадров данных 802.11

## Обзор Высокой Эффективности

Технология Wi-Fi 6 (802.11ax) вся о более лучшем и более эффективном управлении существующей радио частотной среды. Более высокие скорости передачи данных и более широкие каналы не являются целью 802.11ax. Большинство улучшений 802.11ax на Физическом уровне, и включают новую многопользовательскую версию технологии OFDM, вместо однопользовательской технологии OFDM, уже использующейся радиомодулями 802.11a/g/n/ac. Еще одно значительное изменение Wi-Fi 6 в том, что точка доступа 802.11ax может действительно контролировать передачи и нисходящего канала [downlink] и восходящего канала [uplink] нескольким клиентским радиомодулям, пока ТД контролирует среду. В дополнение к этим улучшениям многопользовательской эффективности, радиомодули Wi-Fi 6 (802.11ax) будут обратно совместимы с радиомодулями 802.11a/b/g/n/ac. Таблица 19.1 показывает верхнеуровневое сравнение характеристик 802.11n, 802.11ac, и 802.11ax. Обратите, пожалуйста, внимание, что в отличие от радиомодулей 802.11ac, которые могут передавать только в 5 ГГц полосе частот, радиомодули 802.11ax могут работать и в 2,4 ГГц и 5 ГГц полосах частот. Как вы узнали в Главе 6 “Беспроводные Сети и Технологии Расширения Спектра”, FCC и другие регулирующие организации открыли частотный спектр 6 ГГц для безлицензионной связи. Уже в 2021 радиомодули 802.11ax, которые передают в полосе 6ГГц, появятся на коммерческом рынке.

**ТАБЛИЦА 19.1** Сравнение 802.11n, 802.11ac, и 802.11ax

|                               | <b>802.11n (Wi-Fi 4)</b>   | <b>802.11ac (Wi-Fi 5)</b>  | <b>802.11ax (Wi-Fi 6)</b>            |
|-------------------------------|----------------------------|----------------------------|--------------------------------------|
| Полосы частот                 | 2.4 ГГц и 5 ГГц            | 5 ГГц только               | 2.4 ГГц, 5 ГГц, и 6 ГГц              |
| Размер канала (МГц)           | 20, 40                     | 20, 40, 80, 80 + 80, и 160 | 20, 40, 80, 80 + 80, и 160           |
| Частотное мультиплексирование | OFDM                       | OFDM                       | OFDM и OFDMA                         |
| Пространство поднесущих (кГц) | 312.5                      | 312.5                      | 78.125                               |
| OFDM символьное время (мкс)   | 3.2                        | 3.2                        | 12.8                                 |
| Защитный интервал (мкс)       | 0.4 или 0.8                | 0.4 или 0.8                | 0.8, 1.6, или 3.2                    |
| Общее символьное время (μs)   | 4.0                        | 3.6 или 4.0                | 13.6, 14.4, или 16.0                 |
| Модуляция                     | BPSK, QPSK, 16-QAM, 64-QAM | BPSK, QPSK, 16-QAM, 64-QAM | BPSK, QPSK, 16-QAM, 64-QAM, 1024-QAM |
| MU-MIMO                       | N/A                        | Downlink                   | Downlink and uplink                  |
| OFDMA                         | N/A                        | N/A                        | Downlink and uplink                  |

Как вы можете видеть в Таблице 19.1, 802.11ax поддерживает 40 МГц, 80 МГц, и 160 МГц каналы. Однако основной объем обсуждений связи Wi-Fi 6 мы сфокусируем на 20 МГц каналах. Собственно говоря, ключевые преимущества 802.11ax будут результатом разделения 20 МГц канала на маленькие под-каналы, использующие многопользовательскую версию OFDM, называемую множественный доступ с ортогональным частотным разделением [orthogonal frequency-division multiple access (OFDMA)].

## МногоПользовательский

Термин *многопользовательский* [*multi-user (MU)*] просто подразумевает, что передачи между ТД и несколькими клиентами могут происходить в одно и то же время, в зависимости от поддерживаемой технологии. Однако, терминология MU может быть очень запутанной при обсуждении 802.11ax. Характеристики MU есть и для

OFDMA и MU-MIMO. Пожалуйста, учитывайте ключевые различия, как объяснено далее в этой главе. 802.11ax определяет использование многопользовательские технологии OFDMA и MU-MIMO. Но, пожалуйста, не путайте OFDMA с MU-MIMO. OFDMA обеспечивает многопользовательский доступ путем разделения канала. MU-MIMO обеспечивает многопользовательский доступ путем использования разных пространственных потоков. Если мы обратимся к аналогии с автомобилем и дорогой, обсуждаемой ранее, то OFDMA использует одну дорогу, разделенную на несколько полос для использования разными автомобилями в одно и то же время, когда MU-MIMO использует разные однополосные дороги, чтобы прибыть в один и тот же пункт назначения.

При обсуждении Wi-Fi 6 часто путаются, потому что многие люди могут быть уже знакомы с технологией MU-MIMO представленной в 802.11ac (Wi-Fi 5). С чем большинство людей не знакомы – так это с многопользовательской технологией OFDMA. Вы узнаете, что большая часть преимуществ эффективности Wi-Fi 6 является результатом многопользовательского OFDMA. Поправка 802.11ax позволяет комбинированное использование многопользовательского OFDMA и MU-MIMO одновременно, но не ожидается, что это будет широко применяться.

## OFDMA

*Множественный доступ с ортогональным частотным разделением [Orthogonal frequency-division multiple access (OFDMA)]* вероятно самая важная новая характеристика Wi-Fi 6. Радиомодули 802.11a/g/n/ac на текущий момент используют мультиплексирование с ортогональным частотным разделением [orthogonal frequency division multiplexing (OFDM)] для однопользовательской передачи на частоте 802.11. Радиомодули Wi-Fi 6 используют множественный доступ с ортогональным частотным разделением [orthogonal frequency division multiple access (OFDMA)], который является многопользовательской версией технологии цифровой модуляции OFDM. OFDMA делит Wi-Fi канал на небольшие блоки частот, которые называются *ресурсными блоками [resource units (RUs)]*, таким образом позволяя точке доступа (ТД) синхронизировать связь (восходящего канала [uplink] и нисходящего канала [downlink]) с несколькими индивидуальными клиентами, назначенными определенным ресурсным блокам (RUs). Путем разделения канала, небольшие кадры могут быть одновременно переданы некоторым пользователям параллельно. Думайте об OFDMA как о технологии, которая делит Wi-Fi канал на небольшие *подканалы [sub-channels]* так, что могут происходить одновременные многопользовательские передачи. Например, традиционный 20 МГц канал может быть разделен на девять небольших подканалов. Используя OFDMA, ТД 802.11ax может одновременно передавать небольшие кадры девяти клиентам 802.11ax. Сертификационная программа СЕРТИФИЦИРОВАННЫЙ Wi-Fi 6 [Wi-Fi CERTIFIED 6] от Wi-Fi Альянса на текущий момент проверяет до четырех ресурсных блоков.

OFDMA намного более эффективно использует среду для небольших кадров. Одновременная передача срезает чрезмерную служебную информацию [overhead] MAC подуровня и накладные расходы [overhead] при борьбе за среду. ТД может занять весь канал для одного пользователя или разделить его для работы с несколькими пользователями одновременно, на основе потребностей клиентского трафика. Цель OFDMA лучше использовать доступное частотное пространство. Технология OFDMA была проверена

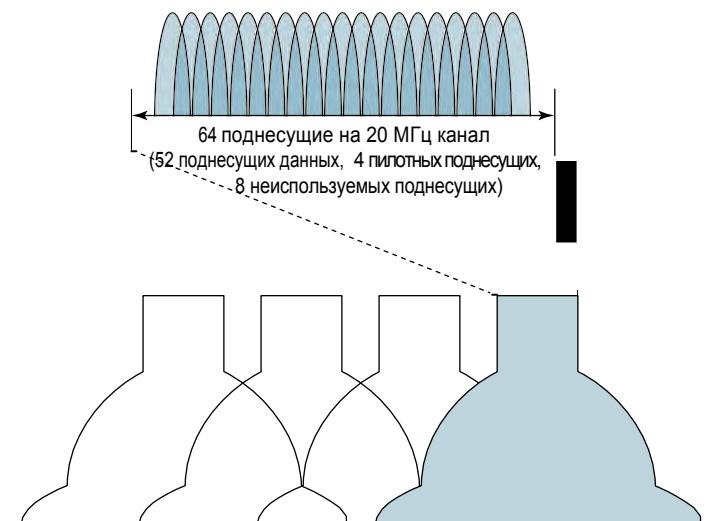
временем в другой радиосвязи. Например, OFDMA используется для нисходящего канала [downlink] сотовой связи LTE. Для обратной совместимости радиомодули 802.11ах будут продолжать поддерживать OFDM. Держите в уме, что кадры управления и контроля 802.11 будут продолжать передаваться на базовых скоростях передачи данных, используя технологию OFDM, которую могут понять радиомодули 802.11a/g/n/ac. Следовательно, передача кадров управления и контроля будет передаваться по всем поднесущим всего основного 20 МГц канала. OFDMA есть только для обмена кадров передачи данных 802.11 между ТД Wi-Fi 6 и клиентами Wi-Fi 6.

## Поднесущие

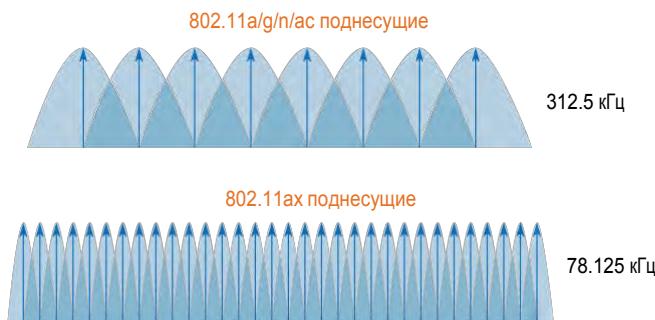
И OFDM, и OFDMA делят канал на поднесущие с помощью математической функции, которая называется *обратное быстрое преобразование Фурье [inverse fast Fourier transform (IFFT)]*. Пространство поднесущих ортогональное, поэтому они не интерфеcируют друг с другом несмотря на недостаточные защитные полосы между ними. Это создает сигнальные нули [signal nulls] в смежных поднесущих частотах, таким образом предотвращая *интерференцию между несущими [inter-carrier interference (ICI)]*.

Какие ключевые различия между OFDM и OFDMA? Как показано на Рисунке 19.4, 20 МГц канал 802.11n/ac состоит из 64 поднесущих. Пятьдесят две поднесущих используются для передачи модулированных данных, четыре поднесущих работают в качестве пилотных несущих, а восемь поднесущих выполняют роль защитных полос. OFDM поднесущие иногда называются *OFDM тонами [OFDM tones]*. В этой главе мы будем использовать оба термина взаимозаменяемо. Каждая OFDM поднесущая - 312.5 кГц.

**РИСУНОК 19.4** 20 МГц канал 802.11n/ac—OFDM поднесущие



Вы узнаете позже в этой главе, что 802.11ах ввела более длительное время символа OFDM в 12.8 микросекунды, который в четыре раза длиннее, чем время, устаревшего символа в 3.2 микросекунды. Результат более продолжительного времени символа - размер поднесущей и пространства уменьшился с 312.5 кГц до 78.125 кГц, как показано на Рисунке 19.5. Узкое пространство поднесущей обеспечивает лучшее выравнивание и улучшенную устойчивость канала. Из-за пространства в 78.125 кГц, 20 МГц OFDMA канал всего состоит из 256 поднесущих (тонов).

**РИСУНОК 19.5** Пространство поднесущих

Также как с OFDM, существует три типа поднесущих OFDMA

**Поднесущие Данных [Data Subcarriers]** Эти поднесущие используют те же самые модуляции и схемы кодирования [modulation and coding schemes (MCSs)] как и 802.11ac и две новых MCSs с дополнительной 1024 квадратурно амплитудной модуляцией (1024-QAM).

**Пилотные Поднесущие [Pilot Subcarriers]** Пилотные поднесущие не несут модулированных данных; однако, они используются для синхронизации между приемником и передатчиком.

**Неиспользуемые Поднесущие [Unused Subcarriers]** Оставшиеся неиспользуемые поднесущие в основном используются как защитные несущие или пустые [null] поднесущие против интерференции от смежных каналов или под-каналов.

С OFDMA эти тоны группируются вместе в отдельные подканалы, называемыми ресурсными блоками [resource units (RUs)]. Путем разделения канала, параллельные передачи небольших кадров нескольким пользователям могут происходить одновременно. Поднесущие данных и пилотные поднесущие в каждом ресурсном блоке являются смежными и следующими друг за другом в OFDMA канале.

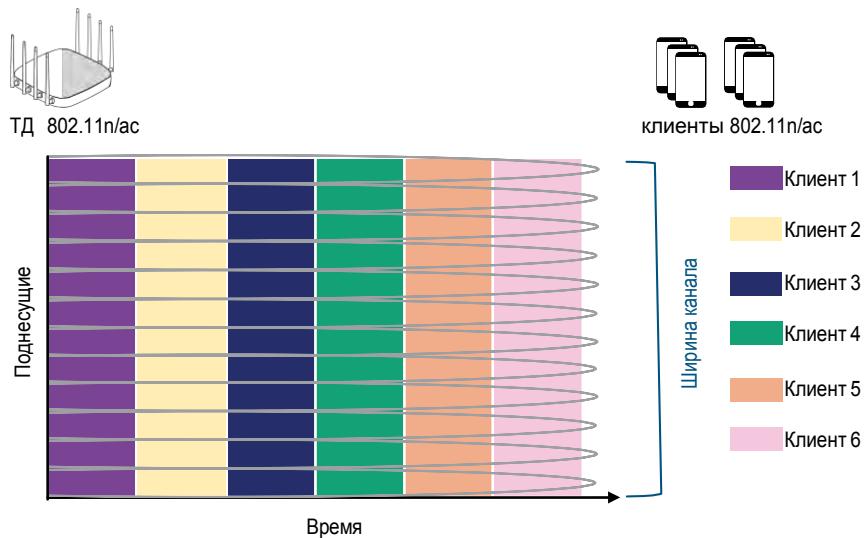
## Ресурсные Блоки

Чтобы еще больше проиллюстрировать разницу между OFDM и OFDMA, обратитесь, пожалуйста, к Рисункам 19.6, 19.7 и 19.8. Когда ТД 802.11n/ac передает в нисходящем канале [downlink] к клиентам 802.11n/ac по OFDM каналу, все частотное пространство канала используется для каждой независимой нисходящей [downlink] передачи. На примере, показанном на Рисунке 19.6, ТД передает шести клиентам независимо все время. При использовании 20 МГц OFDM канала все 53 поднесущие используются для независимой передачи. Другими словами, весь 20 МГц канал нужен для связи между ТД и одним OFDM клиентом. Связь - однопользовательская [single-user]. Тоже самое верно для любой восходящей [uplink] передачи от одного 802.11n/ ac клиента к ТД 802.11n/ac. Весь 20 МГц OFDM канал нужен для клиентской передачи к ТД.

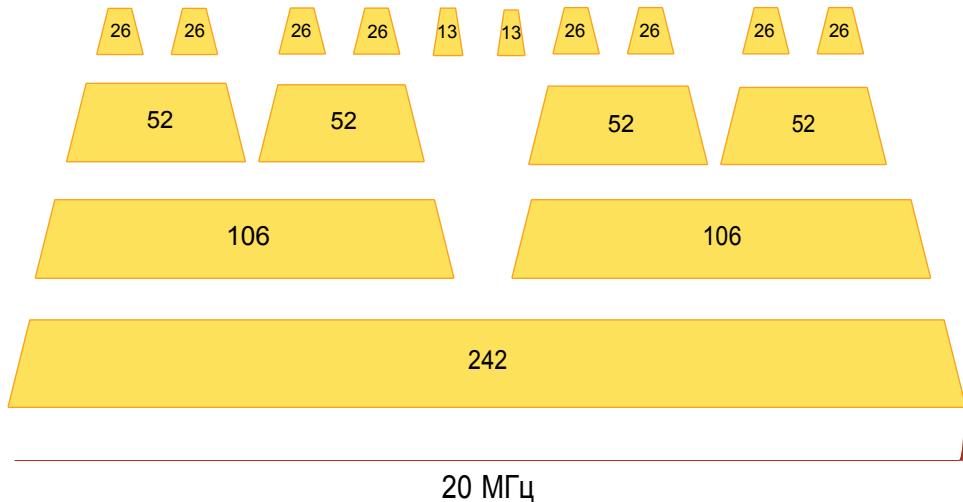
Как ранее утверждалось, канал OFDMA состоит из 256 поднесущих (тонов). Эти тоны сгруппированы в небольшие подканалы, называемые *ресурсными блоками* [resource units (RUs)]. Как показано на Рисунке 19.7, при делении 20 МГц канала, точка доступа 802.11ax назначает поднесущие ресурсные (RUs) 26, 52, 106, и 242, которые примерно соответствуют

каналам 2 МГц, 4 МГц, 8 МГц, и 20 МГц соответственно. ТД 802.11ax указывает сколько RUs используется в 20МГц канале, и различные комбинации, которые могут быть использованы. ТД может занимать целый канал только для одного клиента, или может поделить канал для обслуживания нескольких клиентов одновременно. Например, ТД 802.11ax может одновременно взаимодействовать с одним клиентом 802.11ax, используя 8 МГц частотного пространства, в тоже время взаимодействуя с тремя другими 802.11ax, используя 4 МГц подканалы. Эти одновременные взаимодействия могут быть и в нисходящем канале [downlink] и восходящем канале [uplink].

**РИСУНОК 19.6** OFDM передачи во времени

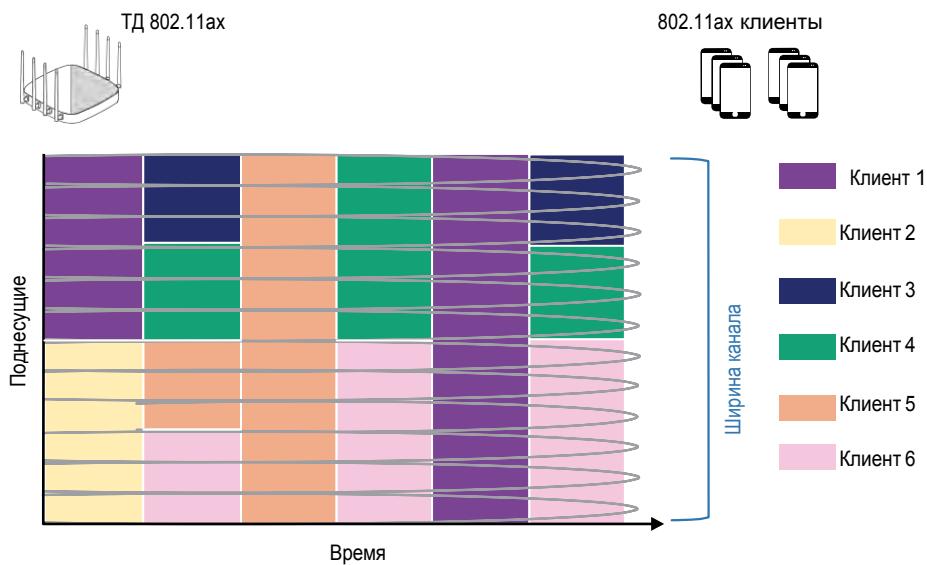


**РИСУНОК 19.7** Ресурсные блоки OFDMA



В примере, показанном на Рисунке 19.8, ТД 802.11ax сначала одновременно передает в нисходящем канале [downlink] 802.11ax клиентам 1 и 2. 20 МГц OFDMA канал фактически поделен на два подканала. Помните, что 20 МГц ODFMA канал имеет всего 256 поднесущих; однако, ТД одновременно передавала клиентам 1 и 2, используя два разных ресурсных блока по 106-тонов. Во второй передаче, ТД одновременно передает в нисходящем канале клиентам 3, 4, 5, и 6. В этом случае, ODFMA канал должен был быть поделен на четыре отдельных подканала по 52 тона. В третьей передаче ТД использовала один ресурсный блок из 242 тонов для нисходящей передачи одному клиенту (клиенту 5). Использование одного ресурсного блока из 242 тонов - это фактически использование всего 20 МГц канала. В четвертой передаче ТД одновременно передает в нисходящем канале клиентам 4 и 6, используя ресурсные блоки по 10 тонов. В пятой передаче ТД снова передает в нисходящем канале только одному клиенту с RU и 242 тонов, использующего весь 20 мГц канал. В шестой передаче ТД одновременно передает в нисходящем канале клиентам 3, 4, и 6. В этом примере, 20 МГц канал поделен на три подканала; два RU по 52 тона используются для клиентов 3 и 4, а RU в 106 тонов используется для клиента 6.

**РИСУНОК 19.8** OFDMA передача во времени



Как показано на Рисунке 19.8, ТД 802.11ax делит 20 МГц OFDMA канал на непрерывной основе для передач нисходящего канала. Позже в этой главе вы узнаете, что ТД 802.11ax может также синхронизировать клиентов 802.11ax для одновременных передач в восходящем канале. Текущее поколение радиомодулей Wi-Fi 6 способны делить 20 МГц канал на четыре ресурсных блока по 52 тона.

OFDMA объединяет разные пользовательские данные внутри 20 МГц канала. ТД назначает RUs ассоциированным клиентам на по-TXOP [рег-TXOP] основе, чтобы максимизировать эффективность скачивания [download] и загрузки [upload]. Мощность передачи может быть подстроена для ресурсных блоков и для нисходящего канала[downlink] и восходящего канала[uplink] для улучшения *отношения сигнал-к-интерференции-плюс-шум [signal-to-interference-plus-noise ratio (SINR)]*.

Стоит отметить, что правила борьбы за среду все еще применяются. ТД все еще должна бороться с устаревшими 802.11 станциями за *возможность передачи [transmission opportunity (TXOP)]*. Когда у ТД есть TXOP, ТД контролирует до девяти Wi-Fi 6 клиентских станций для передач и в нисходящем канале [downlink] и восходящем канале [uplink]. Число используемых RUs может варьироваться на основе TXOP [рег TXOP].

Могут ли ресурсные блоки быть использованы для 40 МГц или 80 МГц каналов? Ответ - да; 40 МГц, 80 МГц и даже 160 МГц каналы также могут быть поделены на различные комбинации RUs, как показано в Таблице 19.2. Если 80 МГц канал был бы поделен только на RU из 26 тонов, то теоретически тридцать семь 802.11ax клиентов могло бы поддерживать связь одновременно с помощью своих возможностей OFDMA. Текущее поколение радиомодулей Wi-Fi 6 способно поделить 80 МГц канал на шестнадцать ресурсных блоков по 52 тона.

Однако, изначально, большинство реальных установок Wi-Fi 6 вероятно будут использовать 20 МГц или 40 МГц каналы с максимумом из четырех клиентов, участвующих в многопользовательских OFDMA передачах на каждую возможность передачи (TXOP). Например, 20 МГц канал поделен на четыре ресурсных блока по 52 тона, или 40 МГц канал поделен на четыре ресурсных блока по 106 тонов. Механизмы выделения и расписания ресурсных блоков вероятно станут более точными в более поздних поколениях чипсетов 802.11ax и прошивок. Помним, что весь смысл OFDMA в использовании небольших подканалов.

**ТАБЛИЦА 19.2** Ресурсные блоки и широкие каналы

| Ресурсный Блок (RU) | 20 МГц Канал | 40 МГц Канал | 80 МГц Канал | 160 МГц Канал | 80 + 80 МГц Канал |
|---------------------|--------------|--------------|--------------|---------------|-------------------|
| 996 (2x) тонов      | н/п          | н/п          | н/п          | 1 клиент      | 1 клиент          |
| 996 тонов           | н/п          | н/п          | 1 клиент     | 2 клиента     | 2 клиента         |
| 484 тона            | н/п          | 1 клиент     | 2 клиента    | 4 клиента     | 4 клиента         |
| 242 тона            | 1 клиент     | 2 клиента    | 4 клиента    | 8 клиентов    | 8 клиентов        |
| 106 тонов           | 2 клиента    | 4 клиента    | 8 клиентов   | 16 клиентов   | 16 клиентов       |
| 52 тона             | 4 клиента    | 8 клиентов   | 16 клиентов  | 32 клиента    | 32 клиента        |
| 26 тонов            | 9 клиентов   | 18 клиентов  | 37 клиентов  | 74 клиента    | 74 клиента        |

## Триггерные кадры

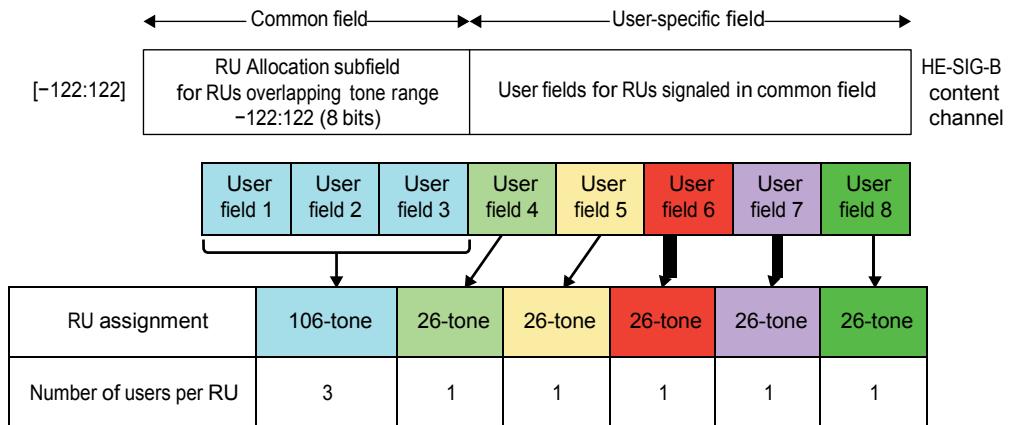
Когда ссылаются на передачи в нисходящем [downlink] и восходящем [uplink] каналах часто используют акронимы DL-OFDMA и UL-OFDMA. В следующих разделах мы узнаем, что серия обмена кадров используется и для DL-OFDMA и UL-OFDMA. В обоих случаях нужны триггерные кадры [*trigger frames*] для обеспечения необходимомого обмена кадрами для многопользовательской связи. Например, триггерный кадр используется для назначения ресурсных блоков (RUs) OFDMA клиентам Wi-Fi 6. Несколько типов контрольных кадров 802.11 может работать как триггерные кадры, как показано в Таблице 19.3.

**ТАБЛИЦА 19.3** Триггерные кадры

| Значение Под поля Типа Триггера | Вариант Триггерного Кадра                           |
|---------------------------------|-----------------------------------------------------|
| 0                               | Базовый [Basic]                                     |
| 1<br>report poll (BRP)]         | Опрос отчета о формировании луча [Beamforming       |
| 2                               | MU-BAR                                              |
| 3                               | MU-RTS                                              |
| 4<br>poll (BSRP)]               | Опрос отчета о статусе буфера [Buffer status report |
| 5                               | GCR MU-BAR                                          |
| 6<br>report poll (BQRP)]        | Опрос отчета о запросах полосы [Bandwidth query     |
| 7<br>report poll (NFRP)]        | Опрос отчета об обратной связи NDP [NDP feedback    |
| 8–15                            | Зарезервированы                                     |

Как ранее упоминалось, триггерные кадры содержат информацию о назначении ресурсных блоков (RU). Информация о назначении или выделении RU сообщается клиентам на физическом (PHY) и MAC уровнях. На Физическом уровне, информация о выделении RU может быть найдена в поле *HE-SIG-B* заголовка PHY триггерного кадра 802.11. Поле HE-SIG-B используется для сообщения назначений RU клиентам. Как показано на Рисунке 19.9, поле HE-SIG-B состоит из двух подполей: общее поле [common field] и поле конкретного пользователя [user-specific field]. Подполе общего поля [common field] используется для того, чтобы показать как канал поделен на различные ресурсные блоки [RUs]. Например, 20 МГц канал может быть поделен на один RU из 106 тонов и четыре RU из 26 тонов. Поле конкретного пользователя [user-specific field] состоит из многопользовательских полей, которые используются чтобы сообщить, какой пользователь назначен какому каждомуциальному ресурсному блоку (RU).

**РИСУНОК 19.9** Выделение RU на Физическом(PHY) уровне



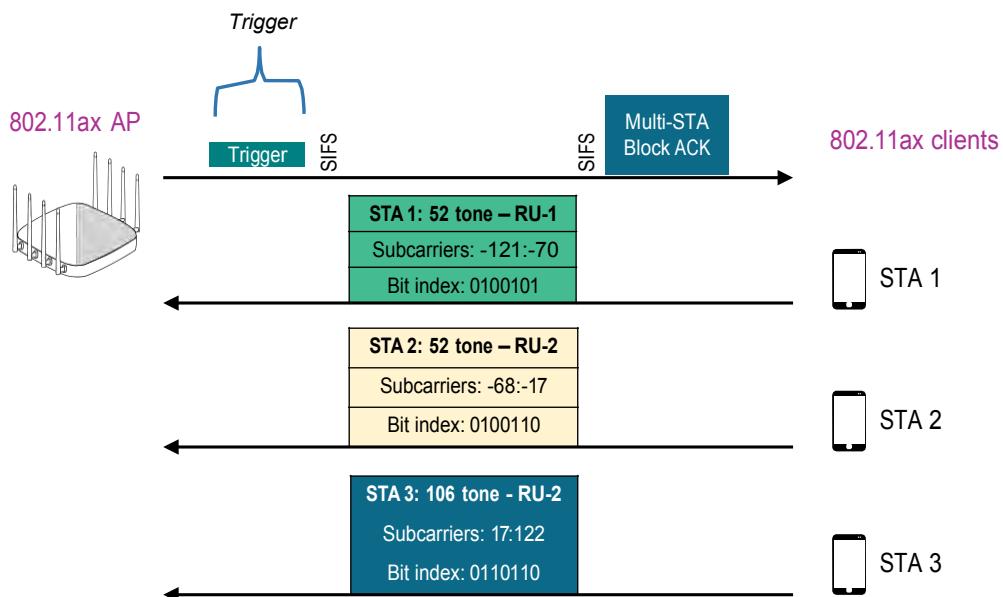
А как информация о выделении RU сообщается на MAC уровне? Информация о выделении RU доставляется в поле *пользовательская информация [user information]* в теле триггерного кадра. Рисунок 19.10 показывает таблицу того, как информация о выделении RU сообщается на MAC уровне. В таблице выделены все возможные RU внутри 20 МГц канала и диапазон поднесущих для каждого RU. Каждый конкретный RU определяется уникальной комбинацией из 7 битов внутри поля пользовательской информации триггерного кадра, которые называются биты назначения RU [RU allocation bits].

**РИСУНОК 19.10** Выделение RU на MAC уровне

| 26 tone RU         | RU-1           | RU-2    | RU-3    | RU-4    | RU-5        | RU-6    | RU-7    | RU-8    | RU-9    |
|--------------------|----------------|---------|---------|---------|-------------|---------|---------|---------|---------|
| Subcarrier range   | -121:-96       | -95:-70 | -68:-43 | -42:-17 | 16:-4, 4:16 | 17:42   | 43:68   | 70:95   | 96:121  |
| RU allocation bits | 0000000        | 0000001 | 0000010 | 0000011 | 0000100     | 0000101 | 0000110 | 0000111 | 0001000 |
| <hr/>              |                |         |         |         |             |         |         |         |         |
| 52 tone RU         | RU-1           | RU-2    |         |         | RU-3        | RU-4    |         |         |         |
| Subcarrier range   | -121:-70       |         | -68:-17 |         |             |         | 17:68   | 70:121  |         |
| RU allocation bits | 0100101        |         | 0100110 |         |             |         | 0100111 | 0101000 |         |
| <hr/>              |                |         |         |         |             |         |         |         |         |
| 106 tone RU        | RU-1           |         |         |         | RU-2        |         |         |         |         |
| Subcarrier range   | -122:-17       |         |         |         | 17:122      |         |         |         |         |
| RU allocation bits | 0110101        |         |         |         | 0110110     |         |         |         |         |
| <hr/>              |                |         |         |         |             |         |         |         |         |
| 242 tone RU        | RU-1           |         |         |         |             |         |         |         |         |
| Subcarrier range   | -122:-2, 2:122 |         |         |         |             |         |         |         |         |
| RU allocation bits | 0111101        |         |         |         |             |         |         |         |         |

На примере на Рисунке 19.11, триггерный кадр выделяет конкретные ресурсные блоки (RUs) трем клиентским станциям для одновременной передачи в восходящем канале [uplink] в 20 МГц OFDMA канале. Клиентам STA-1 и STA-2 каждому назначены RU по 52 тона, а клиенту STA-3 назначен RU из 106 тонов.

**РИСУНОК 19.11** Выделение RU в триггерном кадре



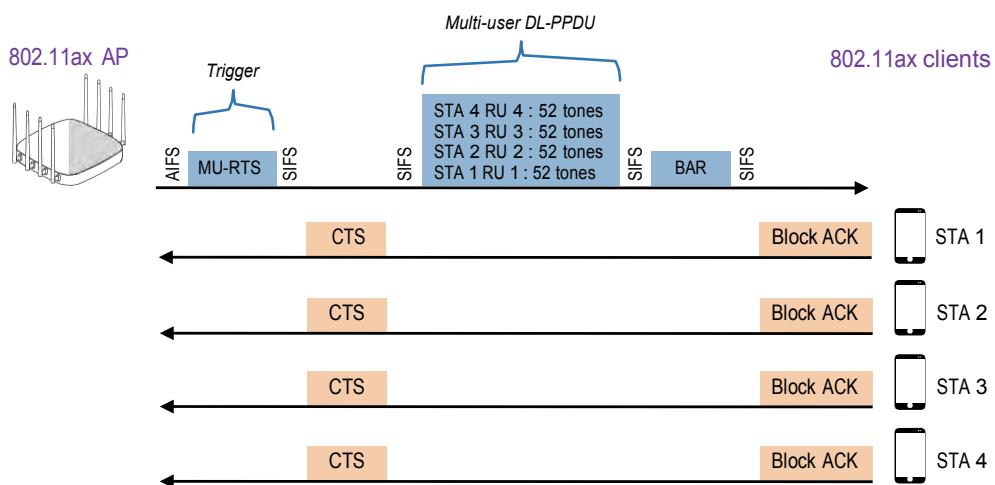
Для UL-OFDMA, триггерный кадр, отправленный ТД, также используется, чтобы сказать клиентам сколько пространственных потоков и какая модуляция и схема кодирования (MCS) используется при передаче в восходящем канале [uplink] на своих заданных ресурсных блоках (RUs). Эта информация может быть найдена в подполях SS Назначения [SS Allocation] и UL MCS поля пользовательской информации в теле триггерного кадра. Триггерные кадры также могут быть использованы ТД, чтобы сообщить клиентам, чтобы они подстроили свои настройки мощности для синхронизированных передач в восходящем канале. Внутри триггерного кадра, подполе Целевого RSSI восходящего канала [UL Target RSSI] показывает в дБм значение ожидаемой принимаемой мощности на ТД на всех антенах, для передач выделенного ресурсного блока (RU) от восходящих каналов клиентов 802.11ax. Подполе UL Target RSSI использует значения от 0 до 90, которые напрямую соответствуют от -110 дБм до -20 дБм. Значение 127 показывает клиентской станции, чтобы передавать на своей максимальной мощности для назначеннной MCS. На основе этой информации, предоставленной триггерным кадром, мощность передачи может быть подстроена клиентами в восходящем канале [uplink]. Заметьте, что клиентские станции Wi-Fi 6 могут быть не способны удовлетворить целевой RSSI из-за своих аппаратных или регуляторных ограничений.

## OFDMA в нисходящем канале

Давайте сначала взглянем как многопользовательская связь DL-OFDMA может происходить между ТД 802.11ax и клиентами 802.11ax. Пожалуйста, вспомните, что OFDMA предназначен только для обмена кадрами данных 802.11 между ТД 802.11ax и клиентами 802.11ax. ТД 802.11ax сначала нужно побороться за среду и выиграть возможность передачи (TXOP) для всего обмена кадрами DL-OFDMA. Как показано на Рисунке 19.12, если ТД 802.11ax выиграла TXOP, ТД может послать кадр многопользовательского запроса-на- отправку [multi- user request-to-send (MU-RTS)]. Кадр MU-RTS имеет два назначения:

- **Резервирование среды [Reserve the medium]:** Кадр MU-RTS передается с помощью OFDM (не OFDMA) по всему 20 МГц каналу так, чтобы устаревшие клиенты также могли понять MU- RTS. Параметр длительности[duration] кадра MU-RTS необходим для резервирования среды и переустановки таймеров NAV у всех устаревших клиентов для оставшегося обмена кадрами DL-OFDMA. Устаревшие клиенты должны оставаться молчащими, пока передаются многопользовательские OFDMA кадры данных между ТД Wi-Fi 6 и Wi-Fi 6 клиентами.
- **Выделение RU [RU allocation]:** Кадр MU-RTS также является расширенным триггерным кадром ТД, используемым для синхронизационных клиентских ответов готово-к-отправке [clear-to-send (CTS)] в восходящем канале [uplink] для клиентов Wi-Fi 6. ТД использует MU-RTS как триггерный кадр для выделения ресурсных блоков (RUs). Клиенты Wi-Fi 6 отправляют CTS ответы параллельно, используя свои назначенные ресурсные блоки RU.

**РИСУНОК 19.12** OFDMA в нисходящем канале



После параллельного ответа CTS от клиентов, ТД начинает многопользовательские DL- PPDU передачи от ТД к OFDMA-совместимым клиентам. Держите в уме, что ТД определяет, как разделить 20 МГц канал на несколько RUs. Если клиенты Wi-Fi 6 получают свои данные через свои выделенные RUs, им необходимо отправить Блоковое подтверждение [Block ACK] точке доступа.

ТД отправляет кадр запроса Блокового подтверждения [Block ACK request (BAR)], после чего клиенты отвечают Блоковыми подтверждениями [Block ACKs] параллельно. Опционально, клиентами параллельно может быть отправлено автоматическое Block ACK. Если обмен кадрами завершен, ТД или клиенты, которые выиграли следующую TXOP смогут передавать по среде. Однопользовательская связь все еще может поддерживаться для устаревших клиентов. Например, если клиент 802.11n/ac выигрывает следующую возможность передачи (TXOP), то клиент 802.11n/ac отправляет кадр данных в восходящем канале к ТД, используя OFDM.

Но как работает передача в восходящем канале для OFDMA клиентов? В следующем разделе вы узнаете, что ТД должна снова выиграть TXOP, чтобы скоординировать синхронизированную связь UL-OFDMA.

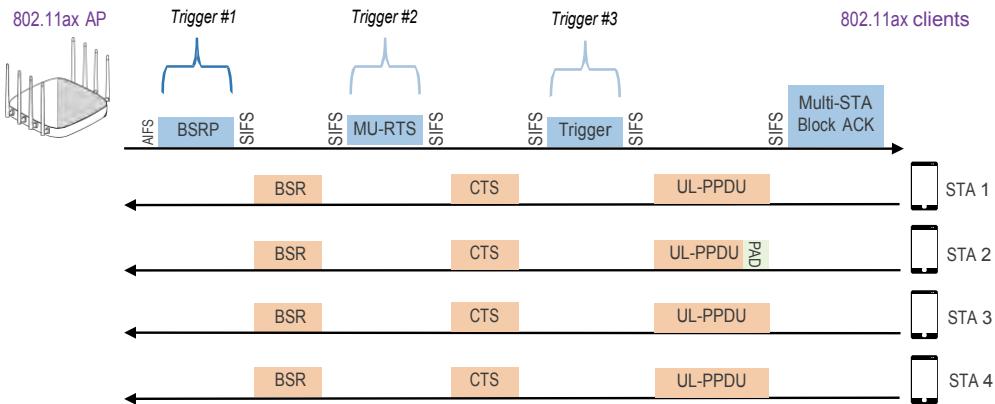
## OFDMA в восходящем канале

В исходном стандарте 802.11 IEEE предлагал рабочий режим с названием *Функция Координации Точной* [Point Coordination Function (PCF)], которая определяла работу, где ТД могла контролировать среду для клиентской передачи в восходящем канале. В режиме PCF, ТД могли бы опрашивать клиентов касательно передач в восходящем канале в периоды времени отсутствия борьбы за среду, когда ТД контролировала среду. Однако, PCF никогда не трогали, и он не был реализован в реальном мире. Сейчас 802.11ax вводит новые механизмы, где ТД может снова контролировать среду для передач в восходящем канале с помощью UL-OFDMA. Нужно понимать, что UL-OFDMA не имеет ничего общего с PCF; методы совершенно разные. Вам следует также понимать, что ТД 802.11ax должна сначала побороться за среду AP и выиграть возможность передачи (TXOP). Если ТД 802.11ax выиграла TXOP, она координирует передачи в восходящем канале от клиентов 802.11ax, которые поддерживают UL-OFDMA.

UL-OFDMA является более сложным, чем DL-OFDMA, и может потребовать использовать до трех триггерных кадров. Каждый триггерный кадр используется для запроса определенного типа ответа от клиентов Wi-Fi 6. UL-OFDMA также требует использование кадров *отчета статуса буфера* [buffer status report (BSR)] от клиентов. Клиенты используют кадры BSR чтобы уведомить ТД о клиентских буферизированных данных и о категориях QoS данных. Информация, содержащаяся в кадрах BSR помогает ТД в выделении ресурсных блоков (RU) для синхронизированных передач в восходящем канале. ТД будет использовать информацию, собранную от клиентов, чтобы построить времена окон в восходящем канале, выделение клиентских ресурсных блоков (RU), и настройки клиентской мощности для каждого RU. Отчеты о статусе буфера [Buffer status reports (BSRs)] могут быть как незапрашиваемые, так и запрашиваемые. Если запрашиваемые, то ТД будет опрашивать клиентов об отчетах BSRs.

Давайте посмотрим на то как происходит многопользовательская UL-OFDMA связь между ТД 802.11ax и клиентами 802.11ax. ТД 802.11ax сначала нужно побороться за среду и выиграть TXOP для всего обмена кадрами UL-OFDMA. Как показано на Рисунке 19.13, если ТД 802.11ax выиграла TXOP, ТД отправит первый триггерный кадр. Кадр опроса отчета о статусе буфера [buffer status report poll (BSRP)] используется для запрашиваемой информации от клиентов 802.11ax об их необходимости в отправке данных в восходящем канале. Затем клиенты отвечают отчетами о статусе буфера [buffer status reports (BSRs)]. Весь смысл в информации BSR в том, что клиенты Wi-Fi 6 помогают ТД Wi-Fi 6 выделить в восходящем канале многопользовательские ресурсы. ТД будет использовать эту информацию для решения как лучше выделить RUs клиентам для передач в восходящем канале.

РИСУНОК 19.13 OFDMA в восходящем канале



Если присутствуют устаревшие клиенты, ТД может отправить кадр многопользовательского запроса-на-отправку [multi-user request-to-send (MU-RTS)], который работает как второй тип триггерных кадров. Процесс RTS/CTS снова используется для резервирования среды только для OFDMA связи. ТД использует MU-RTS в качестве триггерного кадра для выделения ресурсных блоков [resource units (RUs)]. Клиенты 802.11 отправляют ответы CTS параллельно, используя свои назначенные ресурсные блоки (RUs).

Третий и финальный базовый триггерный кадр [*basic trigger frame*] нужен, чтобы дать сигнал клиентам Wi-Fi 6 начать передачу в восходящем канале своих данных в своих назначенных ресурсных блоках (RUs). Базовый триггерный кадр также указывает длину окна в восходящем канале. Клиентские устройства восходящего канала [*uplink*] должны все стартовать и остановиться в одно и то же время. Базовый триггерный кадр также содержит информацию о контроле мощности, так что индивидуальные клиенты могут увеличить или уменьшить свою мощность передачи. Это поможет выровнять мощность приема на ТД от всех клиентов в восходящем канале и улучшить прием. Если данные восходящего канала получены от клиентов, то ТД отправит единое многопользовательское Блоковое подтверждение [*multi-user Block ACK*] клиентам. У ТД также есть опция отправлять отдельные Блоковые подтверждения [*Block ACKs*] каждому индивидуальному клиенту.

Итого: только что обсуждавшийся обмен кадров UL-OFDMA использует три триггерных кадра:

- **Триггер 1:** BSRP для запрашиваемых отчетов о статусе буфера у клиентов.
- **Триггер 2:** MU-RTS для выделения RUs и установки каждого клиентского NAV
- **Триггер 3:** Базовый триггер для подачи сигнала клиентам, чтобы начать свои параллельные передачи в восходящем канале

Стоит понимать, что все три триггерных кадра могут быть нужны, а могут не быть нужны для передачи в восходящем канале. Например, триггерный кадр MU-RTS нужен только в целях механизмов защиты для устаревших клиентов.

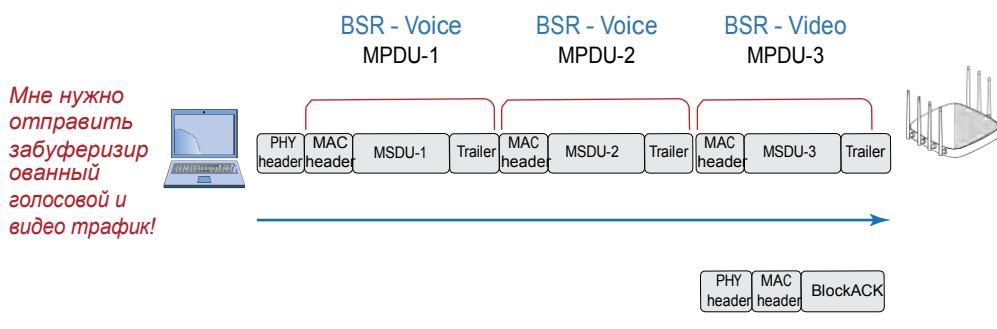
## Отчеты о Статусе Буфера

Как ранее говорилось, ТД Wi-Fi 6 требуют конкретики о состоянии буфера клиента, чтобы произвести соответствующую синхронизацию расписания в восходящем канале. В результате, клиенты Wi-Fi 6 предоставляют BSRs, чтобы помочь ТД в выделении многопользовательских ресурсов в восходящем канале. У клиентов есть два способа доставки

своей информации о состоянии буфера точке доступа. Как ранее обсуждалось, клиенты могут явно [*explicitly*] предоставить BSRs точке доступа в ответ на триггерный кадр BSRP (запрашиваемый BSR). Этот метод проиллюстрирован на Рисунке 19.13. Однако, этот процесс запрашивающего опроса создает накладные расходы [*overhead*] в виде дополнительной служебной информации. Чтобы минимизировать накладные расходы [*overhead*], точка доступа может включить триггерный кадр BSRP вместе с другими кадрами контроля, данных и управления в одном A-MPDU, отправленном клиенту, который поддерживает такую возможность.

Клиенты могут неявно [*implicitly*] предоставить BSRs в поле QoS Control или поле BSR Control любого кадра, переданного точке доступа (незапрашиваемый BSR). Клиенты Wi-Fi 6 могут сообщить незапрашиваемую информацию о статусе буфера для любого выбранного класса QoS трафика в любых кадрах QoS Data или QoS Null, которые они передают. Дополнительно, как показано на Рисунке 19.14, клиент Wi-Fi 6 может сообщить статус буфера нескольких категорий доступа QoS, используя агрегацию кадров A-MPDU кадров QoS Data или QoS Null. Процесс незапрашиваемого BSR более эффективен, потому что он убирает необходимость опроса [polling].

**РИСУНОК 19.14** Незапрашиваемые отчеты статуса буфера и A-MPDU



В дополнение к планируемому по времени UL-OFDMA, 802.11ax предоставляет optionalный метод *случайного доступа UL-OFDMA* [*UL- OFDMA random access (UORA)*]. Метод случайного доступа благоприятен в условиях, когда ТД не знает о буферизированном трафике на клиентах. ТД посыпает триггерный кадр случайного-доступа, чтобы выделить RUs для случайного доступа. Клиенты, которые хотят передать, будут использовать процедуру обратного отсчета OFDMA [*OFDMA back-off (OBO)*]. Изначально, клиент выбирает случайное значение; с каждым триггерным кадром, клиент уменьшает значение на число RUs, указанных в триггерном кадре, пока не достигнет 0. Клиент будет случайным образом выбирать RU и затем передавать.

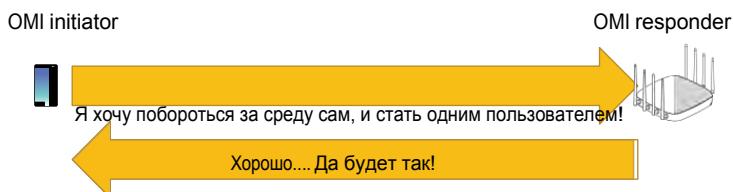
## Индикация Режима Работы

В целях обратной совместимости устаревшие Wi-Fi клиенты 802.11a/b/g/n/ac будут продолжать бороться за среду и выигрывать свои собственные TXOP, если они хотят передавать в восходящем канале. Однако, передачи в восходящем канале Wi-Fi 6 клиентов синхронизованы и контролируются точкой доступа.

Вопрос, который часто задается - “Могут ли клиентские станции Wi-Fi 6 отложить свое участие в синхронизированном восходящем канале OFDMA и побороться за среду за независимую передачу в восходящем канале?”

802.11ax определяет процедуру индикации режима работы [*operating mode indication (OMI)*] для этой цели. Как показано на Рисунке 19.15, клиент Wi-Fi 6, который передает кадр с подполем OM Control определяется как *инициатор OMI* [*OMI initiator*], а ТД - OMI ответчик [*OMI responder*]. Клиент Wi-Fi 6 использует подполе OM Control в кадрах 802.11 данных и управления, чтобы индицировать изменение режима работы или на передачу, или на прием.

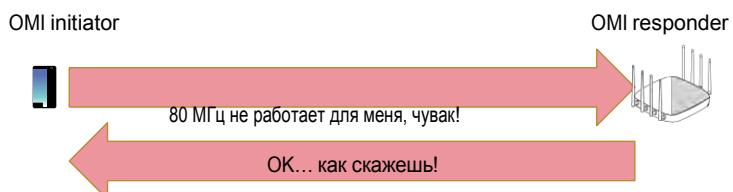
**РИСУНОК 19.15** OMI: Режим работы на передачу



Клиент может переключать между однопользовательской или многопользовательской работой UL-OFDMA с изменением в режиме работы по передаче [*transmit operating mode (TOM)*]. Следовательно, клиент Wi-Fi 6 может и приостановить и продолжить отвечать на триггерные кадры, посылаемые ТД во время процесса UL-OFDMA.

Дополнительно, клиентская станция Wi-Fi может дать сигнал изменения в *режиме работы по передаче [receive operating mode (ROM)]* точке доступа. Клиент показывает ТД максимальное число пространственных потоков и максимальную полосу канала, которую клиент может поддерживать для передачи в нисходящем канале. Как показано на Рисунке 19.16, клиент может показать изменение в размере канала и число поддерживаемых пространственных потоков.

**РИСУНОК 19.16** OMI: Режим работы на прием

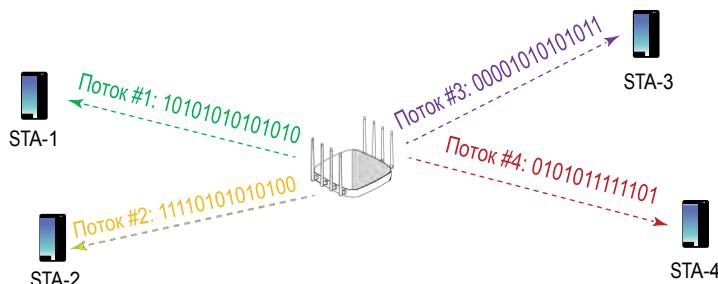


# MU-MIMO

Как вы узнали из Главы 10 “Технология MIMO: НТ и VHT,” возможности нисходящего канала MU-MIMO были представлены во втором поколении точек доступа 802.11ac. В этом разделе мы предоставим небольшое напоминание о технологии MU-MIMO, а также обсудим улучшения MU-MIMO в 802.11ax.

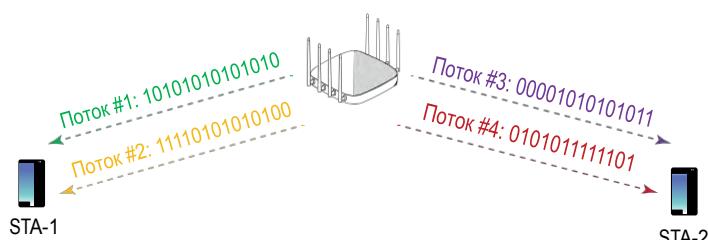
Вторая многопользовательская технология, которую поддерживают радиомодули Wi-Fi 6- это *многопользовательское MIMO [multi-user MIMO (MU-MIMO)]*. Почти также как OFDMA, MU-MIMO поддерживает многопользовательскую связь в нисходящем канале от точки доступа (ТД) нескольким клиентам во время одной и той же возможности передачи (TXOP). Однако, в отличии от разделения частотного пространства, MU-MIMO вместо этого использует преимущества того факта, что ТД имеют несколько радиомодулей и антенн. Как показано на Рисунке 19.17, точка доступа MU-MIMO передает уникальные потоки модулированных данных нескольким клиентам одновременно. Цель в улучшении эффективности путем использования меньшего эфирного времени [airtime].

**РИСУНОК 19.17** MU-MIMO



В Главе 10 мы упомянули, что пятичисленный синтаксис иногда используется при описании возможностей радиомодуля MU-MIMO. Например, когда ТД с поддержкой MU-MIMO, работает используя  $4\times4:4:4$ , четыре уникальных пространственных потока будут направлены четырем независимым клиентам с поддержкой MU-MIMO (см. Рисунок 19.17). Однако, когда ТД с поддержкой MU-MIMO работает как ТД MU-MIMO  $4\times4:4:4:2$ , два уникальных пространственных потока будут назначаться для одного клиента  $2\times2:2$ , а два других пространственных потока будут предназначены другому клиенту  $2\times2:2$  (см. Рисунок 19.18).

**РИСУНОК 19.18** MU-MIMO в нисходящем канале— $4\times4:4:4:2$



Как вы узнали, нисходящий поток [downlink] MU-MIMO был впервые представлен во втором поколении радиомодулей 802.11ac. Однако, очень мало поддерживающих MU-

MIMO 802.11ac (Wi-Fi 5) клиентов присутствует на рынке, и технология редко использовалась на предприятиях. Рисунок 19.19 показывает обзор максимальных клиентских возможностей на корпоративной платформе управления БЛВС. В этом примере, менее 10 процентов клиентов 802.11ac поддерживают MU-MIMO. Однако, эти числа будут расти, потому что клиентская поддержка для нисходящего канала MU-MIMO является обязательным требованием сертификации СЕРТИФИЦИРОВАННЫЙ Wi-Fi 6 [Wi-Fi CERTIFIED 6] от Wi-Fi Альянса.

Ключевая разница между Wi-Fi 5 (802.11ac) MU-MIMO и Wi-Fi 6 MU-MIMO в том, сколько MU-MIMO клиентов взаимодействуют с ТД в одно и тоже время. Wi-Fi 5 ограничен группой MU-MIMO в четыре клиента. Точка доступа Wi-Fi может быть сконструирована для поддержки до 8x8:8 MU-MIMO и в нисходящем и восходящем каналах, которые позволяют обслуживать до восьми клиентов одновременно, и обеспечивать значительно большую пропускную способность передачи данных. 802.11ax также определяет optionalное использование MU-MIMO в восходящем канале. Триггерные кадры используются для того, чтобы дать сигнал клиентам 802.11ax участвовать в связи в восходящем канале MU-MIMO. Если MU-MIMO используется и для нисходящего канала [downlink] и для восходящего канала [uplink], минимальный размер RU - 106 поднесущих.

**РИСУНОК 19.19** Клиентская поддержка MU-MIMO

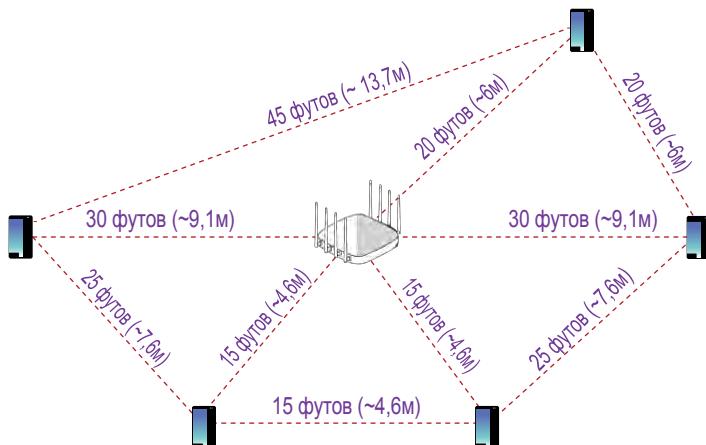


Все Wi-Fi 6 радиомодули первого поколения поддерживают MU-MIMO в нисходящем канале. Поддержка MU-MIMO в восходящем канале может быть добавлена в следующих поколениях оборудования Wi-Fi 6; однако, поддержка будет optionalной.

MU-MIMO также требует формирование луча передачи [transmit beamforming (TxBF)], которое требует исследующих кадров [sounding frames]. Исследующие кадры добавляют избыточную служебную информацию [overhead], особенно когда основной объем кадров данных имеет маленький размер. Дополнительная служебная информация от исследующих кадров [sounding frames] обычно сводит на нет любое увеличение производительности от ТД MU-MIMO, передающей в нисходящем канале одновременно нескольким 802.11ac клиентам. Чтобы решить эту проблему, существуют некоторые улучшения MU-MIMO 802.11ax, включающие группирование исследующих кадров, кадров данных и других кадров от нескольких пользователей, чтобы уменьшить избыточную служебную информацию (оверхед).

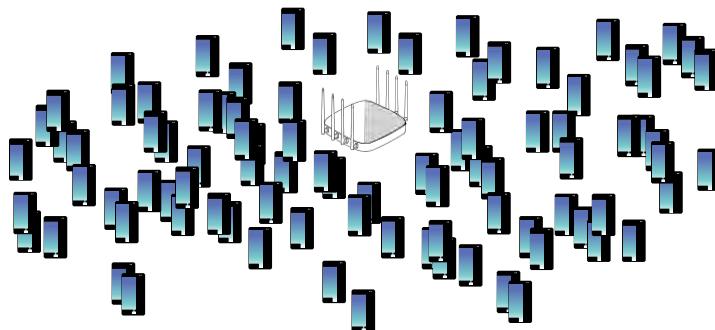
Клиенты Wi-Fi 6 поддерживают MU-MIMO в нисходящем канале [downlink]; однако, MU-MIMO требует пространственного разнесения. Как показано на Рисунке 19.20, необходимо физическое расстояние между клиентами. Дополнительно, MU-MIMO более эффективно, если клиенты остаются стационарными. Даже если все Wi-Fi клиенты поддерживают MU-MIMO, большая часть современных корпоративных установок Wi-Fi включает высокую плотность пользователей и устройств, которая не идеальна для MU-MIMO условий.

**РИСУНОК 19.20** Пространственное разнесение—MU-MIMO



Почти все БЛВС внутри помещений [indoor WLANs] являются средами высокой плотности [high-density (HD)], потому что существует очень много пользователей и очень много устройств. Многие пользователи хотят подключиться к корпоративной БЛВС тремя или четырьмя Wi-Fi устройствами. Большинство сред высокой плотности состоит из нескольких областей, где роуминг также является высшим приоритетом; следовательно, клиенты мобильны и не стационарны. Требуемое пространственное разнесение просто не существует в большинстве корпоративных установок Wi-Fi внутри помещений, как показано на Рисунке 19.21.

**РИСУНОК 19.21** Корпоративная установка Wi-Fi высокой плотности



Очень хороший пример использования MU-MIMO – это мосты точка-многоточка между зданиями (см. Рисунок 19.22). Пространственное разнесение, которое требуется для MU-MIMO, присутствует в этом типе наружных [outdoor] установок. Уличные ТД-мосты также являются стационарными. Для транзитной связи между зданиями, каналы связи –мосты требуют большую ширину полосы, которую может обеспечить MU-MIMO в PtMP установке.

**РИСУНОК 19.22** MU-MIMO с мостами точка-многоточка (PtMP)



Так как же две многопользовательские технологии Wi-Fi 6 соотносятся друг с другом? В теории, MU-MIMO была бы подходящим вариантом в среде с очень низкой клиентской плотностью, но с высокими полосами пропускания. В идеальных условиях, MU-MIMO может улучшить эффективность, когда используются большие пакеты и приложения, требующие большой полосы. Однако, OFDMA это многопользовательская технология, которая будет применяться намного более широко. Wi-Fi 6 позволяет одновременное использование и MU-OFDMA и MU-MIMO, но не ожидается, что это будет широко применяться.

Таблица 19.4 показывает краткое сравнение потенциальных преимуществ MU-MIMO, при сравнении с OFDMA.

**ТАБЛИЦА 19.4** Сравнение OFDMA с MU-MIMO

| OFDMA                                     | MU-MIMO                                                |
|-------------------------------------------|--------------------------------------------------------|
| Увеличенная эффективность                 | Увеличенная емкость                                    |
| Уменьшенная задержка                      | Более высокие скорости передачи данных на пользователя |
| Лучший для приложений с небольшой полосой | Лучший для приложений с большой полосой                |
| Лучший для небольших пакетов              | Лучший для больших пакетов                             |

Итак, пожалуйста, не путайте OFDMA с MU-MIMO. OFDMA обеспечивает многопользовательский доступ путем разделения канала. MU-MIMO обеспечивает многопользовательский доступ путем использования разных пространственных потоков.

## Цвет BSS и Пространственное переиспользование

В этом разделе вы узнаете о цвете BSS [BSS color] и работе пространственного переиспользования [spatial reuse], у которых есть потенциал уменьшить накладные расходы [overhead] при борьбе за среду.

### OBSS

Как вы узнали из разных глав, Wi-Fi использует радиоволновую связь, которая является полу-дуплексной средой—где только один радиомодуль может передавать в частотном домене в любое выбранное время. Частотный домен - причудливая техническая фраза для канала. Все должны быть по очереди, потому что если все "говорят" в одно и то же время, никакие данные не сообщаются, так как никто не "слушает".

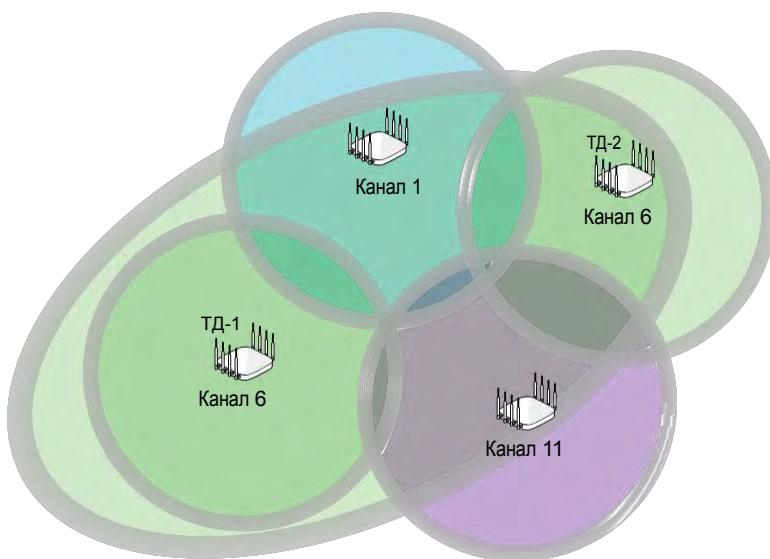
Множественный Доступ с Контролем Несущей и Предотвращением Конфликтов

(CSMA/CA) это метод, используемый в Wi-Fi сетях, чтобы гарантировать, что только один радиомодуль может передавать на одном и том же канале в любое выбранное время.

Радиомодуль 802.11 будет откладывать передачу, если он слышит передачу преамбулы физического уровня [physical (PHY) preamble] любого другого радиомодуля 802.11 с порогом обнаружения сигнала [signal detect (SD)] в 4 децибела или более над уровнем шума. CSMA/CA необходим для предотвращения конфликтов; однако, откладывание передач также потребляет ценное эфирное время.

Эта проблема называется как накладные расходы борьбы (или оверхед борьбы) [*contention overhead*]. Ненужные накладные расходы при борьбе за среду, которые происходят, когда слишком много ТД и клиентов слышат друг друга на одном и том же канале, называется перекрывающийся базовый состав сервиса [*overlapping basic service set (OBSS)*], показанных на Рисунке 19.23. OBSS также обычно называют как одноканальная интерференция [*co-channel interference*].

**РИСУНОК 19.23** OBSS—перекрывающийся базовый состав сервиса

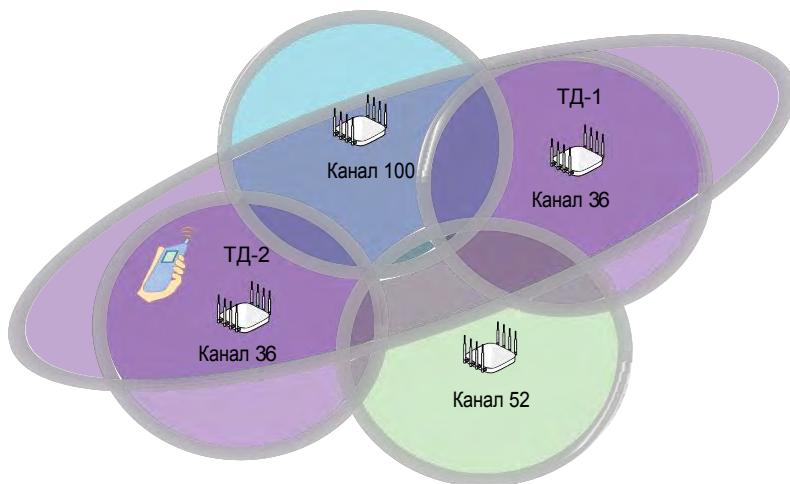


Например, если ТД-1 на канале 6 слышит передачу преамбулы соседней ТД (ТД-2), также передающей на канале 6, то ТД-1 задерживает передачу и не может передавать в одно и то же время. Таким же образом все клиенты, ассоциированные с ТД-1, должны также отложить передачу, если они слышат передачу преамбулы ТД-2. Базовый состав сервиса [*basic service set (BSS)*] - является фундаментальной топологией Wi-Fi сетей.

Взаимодействующие устройства, которые образуют BSS, - это один радиомодуль ТД с одной или более клиентскими станциями. OBSS создает накладные расходы[*overhead*] при борьбе за среду и потребляет ценное эфирное время [*airtime*], потому что у вас два базовых состава сервиса на одном и том же канале, которые могут слышать друг друга—поэтому термин OBSS.

Для повторения того, что вы узнали из предыдущих глав, Wi-Fi клиенты являются основной причиной интерференции OBSS. Из-за мобильной природы клиентских устройств Wi-Fi, интерференция OBSS не является статичной и изменяется по мере движения клиентского устройства. Как показано на Рисунке 19.24, если клиенты, ассоциированные с ТД-2, передают на канале 36, то возможно, что ТД-1 (и все клиенты, ассоциированные с ТД-1) услышат PHY преамбулу клиента и должны будут задержать передачи.

РИСУНОК 19.24 Интерференция OBSS, вызванная Wi-Fi клиентом



## Цвет BSS

В главе 13 "Концепции Проектирования БЛВС" вы узнали, что основной целью модели переиспользования каналов является минимизация потребления эфирного времени [airtime] и уменьшение одноканальной [co-channel] интерференции (также называемой OBSS). План переиспользования каналов уменьшает потребление эфирного времени, вызванного OBSS, путем изоляции частотных доменов. Однако, так как в полосе 2, 4 ГГц доступно только три канала и так как OBSS вызывается клиентами, задержка передач при борьбе за среду практически неизбежна в полосе 2,4 ГГц. OBSS также является проблемой в полосе 5 ГГц, особенно, если много 5 ГГц каналов не доступно для плана переиспользования каналов в 5 ГГц. Чтобы увеличить емкость в плотных средах, частотное переиспользование между базовыми составами сервисов должно быть увеличено. Но существует ли новый способ, который возможно поможет уменьшить OBSS интерференцию?

Стандарт IEEE 802.11ax определяет метод, который может увеличить переиспользование каналов в восемь раз. *Цвет BSS* [BSS color], также называется как *раскраска BSS* [BSS coloring], это способ решения проблемы с накладными расходами [overhead] при борьбе за среду из-за OBSS. Цвет BSS - это идентификатор базового состава сервиса [basic service set (BSS)]. В действительности, цвет BSS не является цветом, а является числовым идентификатором. Радиомодули Wi-Fi 6 способны различать BSS, используя цвет BSS (числовой идентификатор), когда другие радиомодули передают на одном и том же канале.

Информация цвет BSS сообщается и на уровне PHY и на подуровне MAC. В преамбуле PHY заголовка 802.11ax, поле SIG-A содержит 6-битное поле цвет BSS [BSS color]. Это поле может идентифицировать 63 BSS. Это значит, что устаревшие радиомодули 802.11a/b/g/n/ac не смогут интерпретировать биты цвета, потому что они используют другой формат PHY заголовка.

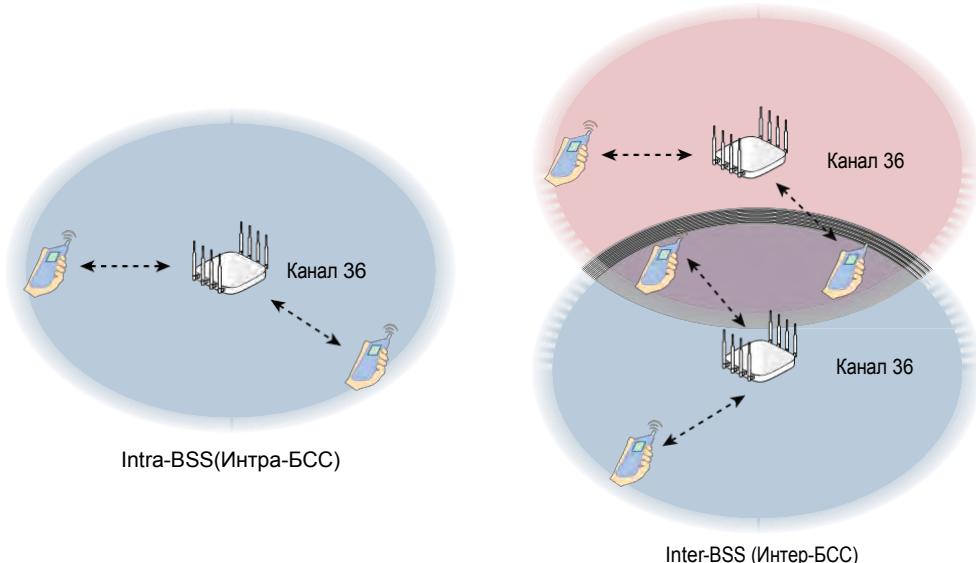
На подуровне MAC, информация цвета BSS видна в кадрах управления 802.11. Информационный элемент работы Высокой Эффективности [HE operation] содержит подполе для информации о цвете BSS. Шесть битов могут быть использованы в качестве идентификации 63 различных цветов (числовых значений) и представлять

различных BSS. Цель в том, чтобы радиомодули 802.11ax различали BSS, используя идентификатор цвета BSS, когда другие радиомодули передают на одном и том же канале.

Как показано на Рисунке 19.25, назначение цвета BSS [BSS color] в том, чтобы уникально идентифицировать разные BSS несмотря на тот факт, что они передают на одном и том же канале. Помните, что этот рисунок - визуальная иллюстрация, и что информация о цвете - это в действительности цифровое значение. Когда радиомодуль Wi-Fi 6 слушает среду и слышит заголовок PHY кадра 802.11ax, отправленного другим радиомодулем Wi-Fi 6, слушающий радиомодуль проверит цвет BSS передающего радиомодуля. Доступ к каналу зависит от обнаруженного цвета:

- **Интра БСС [Intra-BSS]:** Если цвет один и тот же, то кадр считается передачей *внутреннего БСС* или *интра-БСС* [*intra-BSS*] и слушающий радиомодуль отложит по времени передачу.
- **Интер БСС [Inter-BSS]:** Если цвет другой, то кадр считается передачей *внешнего БСС* или *интер-БСС* [*inter-BSS*] от OBSS. Другими словами, передающий радиомодуль принадлежит другому BSS и отсрочка может быть не нужна для слушающего радиомодуля.

**РИСУНОК 19.25** Цвет BSS

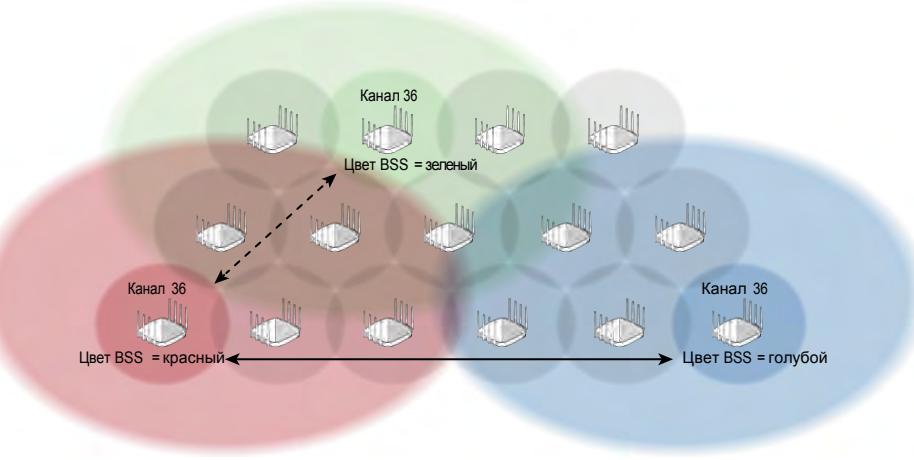


## Работа Пространственного Переиспользования

С помощью процедуры, которая называется *работа пространственного переиспользования* [*spatial reuse operation (SRO)*], радиомодули Wi-Fi 6 будут способны применять пороги адаптивной оценки чистоты канала [*adaptive clear channel assessment (CCA)*] для обнаружения передачи кадров OBSS. Цель цвета BSS [BSS color] и пространственного переиспользования в игнорировании передач от OBSS, и следовательно, быть способным передавать в тоже самое время. На примере, показанном на Рисунке 19.26, трем BSS,

передающие на канале 36, назначены BSS цвета - красный, голубой, и зеленый. Будем это считать интер-БСС [inter-BSS] средой. ТД и клиенты, которые принадлежат красному и зеленому BSS находятся в непосредственной близости друг от друга и вероятнее всего нужна отсрочка по передаче. Однако, несмотря на тот же самый канал, отсрочка по передаче может быть не нужна между ТД и клиентами, которые являются членами красного и голубого BSS. Из-за большего физического расстояния, может быть использован порог адаптивной ССА.

**РИСУНОК 19.26** Интер-БСС [Inter-BSS]



В Главе 8 "Доступ к Среде 802.11" вы узнали, что радиомодули 802.11 используют оценку чистоты канала [*clear channel assessment (CCA)*], чтобы оценить радиосреду. Если радиосреда занята, то радиомодуль 802.11 не будет передавать, а вместо этого отложит на период времени, называемого времем слота [*slot time*]. ССА включает в себя прослушивание радиопередач на Физическом уровне. Радиомодули 802.11 используют два отдельных порога ССА при прослушивании радиосреды. Порог обнаружения сигнала [*signal detect (SD)*] используется для идентификации входящей передачи преамбулы 802.11 от другого передающего радиомодуля 802.11. Преамбула - это компонента заголовка Физического уровня передачи кадров 802.11. Порог обнаружения сигнала [*signal detect (SD)*] статистически около 4 дБ отношения сигнал-шум [*signal-to-noise ratio (SNR)*] для большинства радиомодулей 802.11 для обнаружения и декодирования преамбулы 802.11. Другими словами, радиомодуль 802.11 может обычно декодировать любые входящие передачи преамбулы с принимаемым сигналом около 4 дБ над уровнем шума. Порог обнаружения энергии [*energy detect (ED)*] используется для обнаружения любого типа радио передачи во время оценки чистоты канала [*clear channel assessment (CCA)*]. Порог ED на 20 дБ выше чем порог обнаружения сигнала. Думайте о пороге обнаружения сигнала как о методе обнаружения и отсрочки радиопередачи 802.11. Думайте о пороге обнаружения энергии как о методе обнаружения и отсрочки из-за любых сигналов от не-802.11 передатчиков. Оба порога используются вместе во время ССА, чтобы определить занята ли среда и, следовательно, должна ли быть отсрочка передачи.

Интерференция OBSS является результатом задержки радиосвязи из-за слишком низкого порога обнаружения сигнала [signal detect (SD)]. Статистически, большинство радиомодулей могут декодировать преамбулу 802.11, если принятый сигнал только выше на 4 dB над уровнем шума. Как результат этого очень низкого порога обнаружения сигнала, ТД и клиенты на одном и том же канале слышат друг друга и будут задерживать передачу несмотря на то что они отделены значительной физической дистанцией.

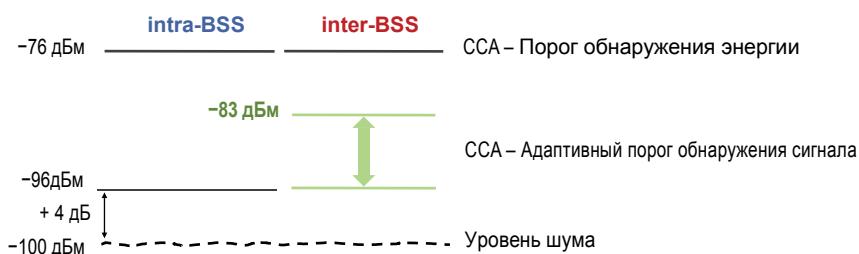
Многие производители корпоративных БЛВС предлагают настройку параметров порогов на ТД, которое называется *старт приема пакетов* [receive start of packet (RX-SOP)]. Эта настройка конфигурации даёт администраторам возможность точной настройки и манипуляции порогом обнаружения сигнала точек доступа. Например, админ может вручную установить менее чувствительный порог SD вместо 4dB над уровнем шума. Менее чувствительный порог SD в результате приведет к уменьшению в одноканальной интерференции [co-channel interference] от ближайших ТД и клиентов на одном и том же канале. К настройке RX-SOP не следует относиться легкомысленно. Если порог поднять слишком высоко, передачи от близких ТД на том же самом канале будут повреждать данные и приводить к деградации производительности, которая в действительности хуже, чем потеря производительности из-за отсрочки из-за OBSS интерференции.

Работа пространственного переиспользования (SRO) позволяет радиомодулям Wi-Fi 6 применять адаптивные пороги обнаружения сигнала оценки чистоты канала (CCA). Думайте об SRO как о динамической реализации настройки статического порога RX-SOP, который может быть установлен вручную админом.

На основе обнаруженного цвета BSS, радиомодули Wi-Fi 6 могут применять адаптивную CCA, которая может поднять порог обнаружения сигнала для кадров интер-БСС [inter-BSS] в тоже время поддерживая более низкий уровень порога для интра-БСС [intra-BSS] трафика. Если порог обнаружения сигнала поднять более высоко для входящих OBSS кадров, радиомодулю может не потребоваться отсрочка, несмотря на тот же самый канал.

Адаптивный порог обнаружения сигнала может быть настроен отдельно для каждого цвета и каждого кадра для интер-БСС [inter-BSS] трафика. На примере в Рисунке 19.27, *статический* [static] порог SD в -96 dBm (децибелы относительно 1 милливатта) может быть использован для приема интра-БСС [intra-BSS] трафика, в то время как *адаптивный* [adaptive] порог SD между -96 dBm и -83 dBm может быть использован для интер-БСС [inter-BSS] трафика.

**РИСУНОК 19.27** Работа пространственного переиспользования—Адаптивный CCA



Цвет BSS вместе с работой пространственного переиспользования имеют потенциал уменьшить проблему борьбы за канал в OBSS, которая является симптомом существующих низких порогов SD. Решит ли цвет BSS проблему одноканальной интерференции [co-channel

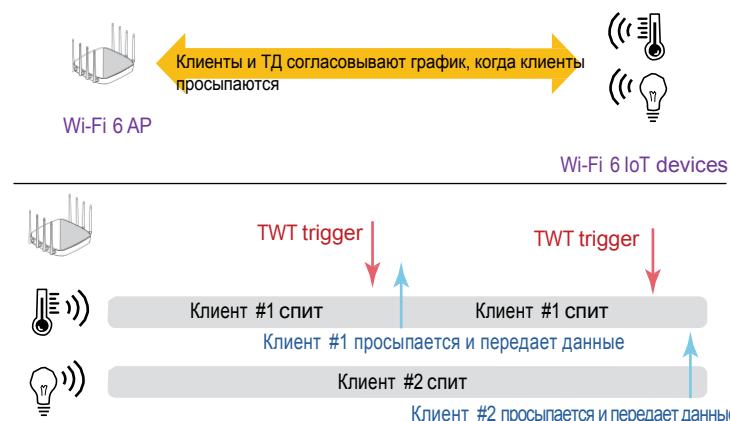
interference]? Ответ - вероятно нет в ближайшее время. Первое, держите в уме, что устаревшие клиенты не умеют различать между BSSами на одном и том же канале. Второе, чтобы адаптивные пороги SD стали правильно работать производителям чипсетов 802.11ax придется еще постараться. Почти также как RX-SOP может быть опасной конфигурационной настройкой, динамические и адаптивные пороги SD могут также иметь негативный эффект. Хотя цвет BSS и SRO имеют потенциал, технологии может понадобится еще долгое время чтобы созреть, прежде чем она будет эффективной в реальной Wi-Fi среде.

## Целевое время пробуждения

*Целевое время пробуждения [Target wake time (TWT)]* - это улучшенный механизм экономии энергии Wi-Fi 6. TWT - это обсуждаемое соглашение, на основе ожидаемой активности трафика между точкой доступа (ТД) и клиентами, чтобы определить планируемое целевое время пробуждения для клиентов Wi-Fi 6 в режиме экономии энергии [power-save (PS)]. Согласовываемые TWTs позволяют ТД управлять клиентской активностью, путем создания расписания работы клиентских станций в разное время для того, чтобы минимизировать борьбу между клиентами. TWT уменьшает количество времени, которое нужно клиентской станции в режиме экономии энергии, чтобы проснуться. Это позволяет клиенту "спать" дольше, и уменьшает потребление энергии. В отличие от механизмов экономии энергии устаревших клиентов, таких как предоставление карты индикации трафика [traffic indication map (DTIM)], которая требует, чтобы спящие клиентские устройства просыпались в микросекундные интервалы, целевое время пробуждения [target wake time (TWT)] может теоретически позволить клиентским устройствам спать часами. TWT - это идеальный метод экономии энергии для IoT устройств, которым нужно беречь время жизни батареи.

Как показано на Рисунке 19.28, обмен кадров TWT используется между ТД и клиентами, чтобы договориться о расписании TWT. Для каждого клиента Wi-Fi 6 может быть до восьми отдельных соглашений по обговариваемым планируемым пробуждениям для разных типов трафика приложений. Когда процесс согласования завершен, клиент засыпает и затем просыпается в заданные (целевые) интервалы. У 802.11ax также есть расширенная функциональность TWT по включению не-согласованного TWT. ТД может создать расписание пробуждения и доставку значений TWT клиентам 802.11ax через процедуру широкого вещания TWT [*broadcast TWT*].

**РИСУНОК 19.28** Целевое время пробуждения



TWT изначально был определен в поправке 802.11ah, которая определяла использование Wi-Fi на частотах ниже 1 ГГц. Вероятное использование 802.11ah - это сети датчиков (или сенсорные сети), вместе с транзитом для сетей датчиков, и Wi-Fi сетей увеличенной дальности. Возможности увеличенной дальности и экономии энергии TWT являются идеальными для устройств Интернета Вещей [*Internet of Things (IoT)*]. Несмотря на цель смешения устройств IoT в полосы с более низкой частотой, большинство IoT устройств с радиомодулем Wi-Fi продолжают передавать в полосе частот 2, 4 ГГц. Так как 802.11ax теперь также определяет TWT, те же самые расширенные возможности по экономии энергии могут быть доступны для устройств IoT с радиомодулями 802.11ax, которые передают в полосе 2,4 ГГц.

Остается посмотреть, будут ли компании устройств IoT производить IoT устройства с радиомодулями 802.11ax; однако, возможность сбережения жизни батареи привлекательна, если устройство поддерживает TWT. Дополнительно, потребляется меньше эфирного времени, если IoT устройства 802.11ax могут спать расширенный период времени. Как ранее упоминалось, сенсорные устройства 802.11ax могут спать часами, оставаясь ассоциированными с ТД. Таблицы ассоциации на ТД могут, следовательно, быть достаточно большими, если IoT устройства расположены вблизи ТД. Любому устройству IoT, которое может спать часами, вероятнее всего нужен будет статический IP адрес, потому что их интервал сна может в реальности превысить интервал выдачи (аренды) IP адреса по DHCP. Статические IP адреса будут нужны, чтобы избежать повторного обмена сообщениями DHCP при выдаче IP адреса, когда просыпается устройство IoT.

## Дополнительные возможности 802.11ax PHY и MAC

OFDMA, MU-MIMO, Цвет BSS, и TWT являются компонентами 802.11ax. Однако, черновая поправка 802.11ax определяет большое количество других характеристик уровней PHY и MAC, которые приведут к лучшей и более эффективной Wi-Fi связи.

### 1024-QAM

Хотя, основная цель 802.11ax в увеличенной эффективности, больше скорости не плохая вещь. Увеличенная эффективность и большая скорость не являются взаимно исключающими целями. Квадратурная Амплитудная Модуляция [Quadrature amplitude modulation (QAM)] использует и фазу, и амплитуду радиоволнового сигнала, чтобы представить биты данных. Радиомодули Wi-Fi 6 поддерживают *1024-QAM* и новые схемы модуляции и кодирования [*modulation and coding schemes (MCSs)*], которые определяют более высокие скорости передачи данных.

Как обсуждалось в ранних главах, диаграмма созвездий, также называемая как карта созвездий, - это двухмерная диаграмма, часто используемая для представления модуляции QAM. Диаграмма созвездий поделена на четыре квадранта, и разные положения в каждом квадранте могут использоваться для представления битов данных. Области в квадранте относительно горизонтальной оси используются для представления различных изменений (сдвигов) фазы. Области относительно вертикальной оси используются для представления изменений амплитуды.

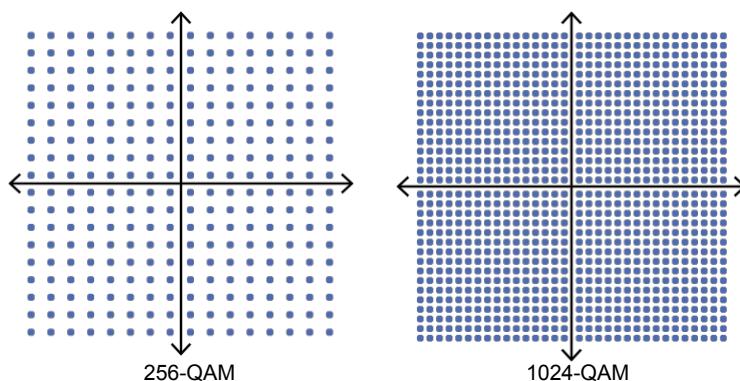
Для сравнения, 256-QAM (представленная в 802.11ac) модулирует 8 бит на символ, когда 1024-QAM модулирует 10 бит на символ—потенциально на 25 процентов больше

в пропускной способности данных. Wi-Fi 6 также вводит две новых MCSs, которые используют модуляцию 1024-QAM: MCS-10 и MCS-11, оба из которых опциональны. По умолчанию, 1024-QAM используется с ресурсными блоками (RUs) из 242 поднесущих. Это означает, что по крайней мере полная 20 МГц полоса канала обычно будет нужна для 1024-QAM. Меньшие RUs могут быть использованы для 1024-QAM, но радиомодули вероятно не будут поддерживать такую возможность.

Почти также, как и для 256-QAM, будут нужны очень высокие пороги отношения сигнал-шум (SNR) (35 децибел или больше) для того, чтобы радиомодули 802.11ax использовали модуляцию 1024-QAM. Вероятнее всего нужна будет нетронутая радиосреда с низким уровнем шума и непосредственная близость между клиентом Wi-Fi 6 и ТД Wi-Fi 6.

Рисунок 19.29 показывает сравнение графиков созвездий [constellation] между модуляциями 256-QAM и 1024-QAM. Как вы видите, у 1024-QAM намного больше точек созвездий. *Величина вектора ошибок* [Error vector magnitude (EVM)] - это мера, используемая для количественной оценки производительности радиоприемника или передатчика относительно точности модуляции. В модуляции QAM, EVM - это мера того, как далеко находится принимаемый сигнал от точки созвездия. Любому радиомодулю 802.11ax, который использует модуляцию 1024-QAM, нужны будут сильные характеристики EVM и приемной чувствительности.

**РИСУНОК 19.29** 256-QAM и 1024-QAM



## Длинное Символьное Время и Защитные Интервалы

Для цифровых сигналов, данные модулируются в несущий сигнал в битах или наборы битов, называемые *символами* [symbols]. 802.11ax представил увеличенное *время символа OFDM* [OFDM symbol time] в 12.8  $\mu$ s (микросекунд), которое в четыре раза больше старого времени символа в 3.2  $\mu$ s (мкс). Увеличение в числе поднесущих (тонов) также увеличивает длительность символа OFDM. Пространство поднесущей обратно пропорционально времени символа. Используемое время символа в четыре раза дольше, поскольку 802.11ax использует пространство поднесущих в 78.125 кГц, которое является одной-четвертой размера старого пространства поднесущих 802.11n/ac.

Из обзора Главы 10, защитный интервал [*guard interval (GI)*] – это период времени между символами, который собирает задержавшиеся с прибытием символы по длинным путям. В среде с многолучевым распространением, символы идут разными путями, поэтому некоторые символы приходят позже. “Новый” символ может прибыть на приемник раньше, чем “запоздавший” символ будет полностью принят. Это называется межсимвольной интерференцией [*intersymbol interference (ISI)*] и может привести к повреждению данных. *Разброс задержки [delay spread]* – это разница во времени между несколькими путями одного и того же сигнала. Нормальный разброс задержки [*delay spread*] составляет от 50 наносекунд до 100 наносекунд, а максимальный разброс задержки около 200 наносекунд. Защитный интервал должен быть от двух до четырех раз длиннее разброса задержки. Думайте о защитном интервале как о буфере для разброса задержки.

802.11a/g определяет использование защитного интервала (GI) в 0.8  $\mu\text{s}$ (мкс) (800 наносекунд), когда 802.11n/ac еще добавляет вариант для короткого защитного интервала в 0.4  $\mu\text{s}$  (400 наносекунд), который был предназначен для использования в средах внутри помещений [*indoor environments*]. Когда старое время символа 3.2  $\mu\text{s}$ , которое используется для модулированных данных, объединяется со стандартным защитным интервалом в 0.8  $\mu\text{s}$ , суммарная продолжительность символа составляет 4.0  $\mu\text{s}$ . Когда старое символьное время 3.2  $\mu\text{s}$  объединяется с коротким защитным интервалом в 0.4  $\mu\text{s}$ , суммарная продолжительность символа равна 3.6  $\mu\text{s}$ .

802.11ax определяет три различных защитных интервала, которые могут использоваться вместе с символьным временем в 12.8  $\mu\text{s}$ , которое используется для модулированных данных:

**Защитный интервал 0,8 мкс [0.8  $\mu\text{s}$  Guard Interval]** Этот защитный интервал вероятно будет использоваться для большинства сред внутри помещений. При объединении со временем в 12,8 мкс, которое используется для данных, суммарное символьное время для связи внутри помещений будет 13,6 мкс.

**Защитный интервал 1,6 мкс [1.6  $\mu\text{s}$  Guard Interval]** Этот защитный интервал предназначен для связи вне помещений [*outdoor*]. При объединении со временем 12,8 мкс, которое используется для данных, суммарное символьное время будет 14,4 мкс. Защитный интервал может быть необходим в средах в помещениях с высоким многолучевым распространением, чтобы гарантировать стабильность связи в восходящем канале [*uplink*] MU-OFDMA или восходящем канале MU-MIMO.

**Защитный интервал 3,2 мкс [3.2  $\mu\text{s}$  Guard Interval]** Этот защитный интервал также предназначен для связи вне помещений [*outdoor*]. При объединении со временем в 12,8 мкс, которое используется для данных, суммарное символьное время будет 16,0 мкс. Более длительное символьное время и более длительный защитный интервал обеспечат более надежную связь вне помещений.

## Заголовки PHY 802.11ax

Поправка 802.11ax определяет четыре формата блока данных протокола *PLCP* [*PLCP protocol data unit (PPDU)*]. Простыми словами, существует четыре новых PHY заголовка и преамбул для радиопередач высокой эффективности [*high efficiency (HE)*]. Преамбула используется для синхронизации между передающим и принимающим радиомодулями и состоит из двух частей: устаревшей [*legacy*] и высокой эффективностью [*high efficiency (HE)*]. Устаревшая преамбула просто декодируется устаревшими станциями (STAs) и включена для обратной совместимости. Компоненты преамбулы высокой

эффективности (HE) используются для сообщения информации между радиомодулями Wi-Fi 6 об OFDMA, MU-MIMO, цвете BSS, и так далее.

Как показано на Рисунке 19.30, устаревшие тренировочные поля [legacy training fields] добавляются к заголовку PHY HE чтобы разрешить обратную совместимость с устаревшими радиомодулями 802.11/a/b/g/n/ac, которые используют другой формат PHY. Четыре PPDU 802.11ax PPDUs:

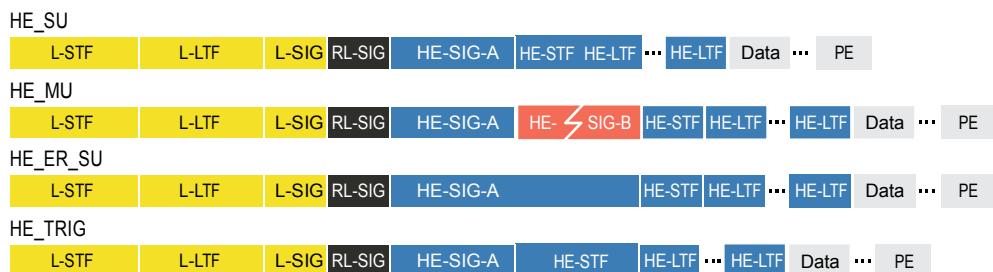
**HE SU** Однопользовательский заголовок PHY высокой эффективности [high efficiency single-user PHY header] используется для однопользовательской передачи.

**HE MU** Многопользовательский заголовок PHY высокой эффективности [high efficiency multi-user PHY header] используется для передачи одному или более пользователям. Заметьте, что этот формат PPDU содержит поле HE-SIG-B, которое нужно и для MU-MIMO и для MU-OFDMA, и выделения ресурсного блока. Этот формат не используется в качестве ответа на триггер, что означает, что этот формат заголовка PHY используется для триггерных кадров или передачи в нисходящем канале [downlink].

**HE ER SU** Однопользовательский формат высокой эффективности увеличенной дальности [high efficiency extended-range single-user format] предназначен для одного пользователя. Части этого заголовка PHY поднимаются на Здецибела, чтобы улучшить связь и дальность вне помещений.

**HE TB** Формат высокой эффективности на основе триггера [high efficiency trigger-based] для передачи, которая является ответом на триггерный кадр. Другими словами, этот формат заголовка PHY используется для связи в восходящем канале [uplink].

#### РИСУНОК 19 .30 Форматы PPDU Высокой Эффективности (HE PPDU)



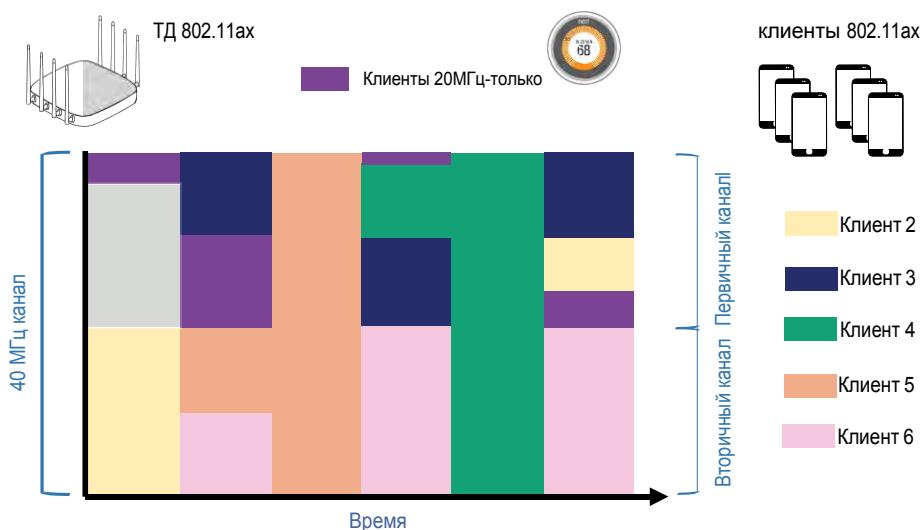
Поле HE-SIG-A во всех четырех заголовках PHY содержит информацию, необходимую для интерпретации HE PPDUs. Различные биты в этом поле заголовка PHY используются для обозначения этой информации. Например, поле SIG-A может показывать является ли передача в восходящем канале [uplink] или в нисходящем канале [downlink]. Информация о модуляции и схеме кодирования, информация о цвете BSS, размер защитного интервала, и многое другое содержится в этом поле заголовка PHY.

## Только-20 МГц

Некоторые радиомодули клиентов Wi-Fi 6 могут воспользоваться преимуществом работы режима только-20МГц [20 MHz-only]. Клиентские станции смогут информировать ТД, что они работают, как только-20МГц клиенты [20 MHz-only clients].

Как показано на Рисунке 19.31, только-20 МГц клиент [20 MHz-only client] все еще может работать на 40 МГц и 80 МГц каналах. Однако, с одним редким исключением в работе, только-20 МГц клиенты должны работать через RUs первичного канала.

**РИСУНОК 19.31** Только-20МГц клиент Wi-Fi 6



Что это фактически значит - а то, что клиенты поддерживают только определенное соответствие [mapping] тонов ресурсным блокам OFDMA. Если ТД передает на стандартном 20 МГц канале, то только-20 МГц клиент очевидно будет способен поддержать тоновое соответствие в ресурсный блок (RU) из 26 тонов, RU из 52 тонов, RU из 106 тонов, и RU из 242 тонов в 20 МГц канале. Если ТД передает на 40 МГц канале, только-20 МГц клиент сможет поддержать только 40 МГц тоновое соответствие в RU из 26 тонов, RU из 52 тонов, или RU из 106 тонов в *первичном канале* [primary channel]. Очень специфичное тоновое соответствие в ресурсный блок (RU) из 26 тонов, RU из 52 тонов, или RU из 106 тонов также поддерживается для только-20МГц клиента, если ТД передает на 80 МГц канале или на 160 МГц канале. Для любых каналов больше чем 20 МГц, RU из 242 тонов является опциональным для только-20МГц клиентов.

Вся задача этих правил в том, чтобы гарантировать, что только-20МГц клиенту назначены соответствия тонов OFDMA и назначений RU, которые клиент может поддержать, даже если используются большие каналы. В отличие от клиентских устройств, типа смартфон или ноутбук, только-20МГц клиенты будут иметь маленький форм фактор с ограниченными вычислительными возможностями и требованиями к низкой мощности. Рабочий режим только-20МГц идеален для IoT клиентов, которые могут также использовать преимущества возможности экономии энергии TWT, но не обязательно нужно иметь все возможности, которые предлагает 802.11ax. Это позволит производителям клиентов создать менее сложные чипсеты с меньшей стоимостью, которые идеальны для IoT устройств.

## AMPDU со Множеством Идентификаторов Трафика (Multi-TID AMPDU)

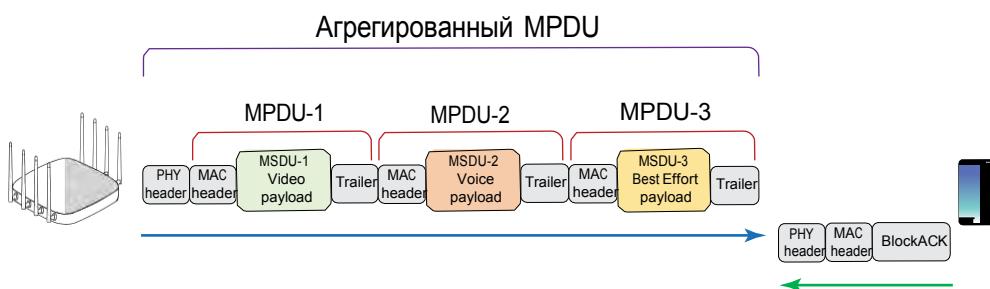
Как вы узнали в ранних главах, два термина, которые все должны понимать это MSDU и MPDU. Блок Сервисных Данных MAC 802.11 [802.11 MAC Service Data Unit (MSDU)] - это полезная нагрузка уровней 3-7 кадра данных 802.11. Блок Данных Протокола MAC 802.11 [802.11 MAC Protocol Data Unit (MPDU)] это, фактически, технический термин для беспроводного кадра. MPDU состоит из заголовка, тела и окончания кадра с полезной нагрузкой MSDU, инкапсулированной в тело кадра.

Агрегация кадров - это метод объединения нескольких кадров в одну передачу кадра. Фиксированная часть служебной информации [overhead] MAC уровня и часть накладных расходов [overhead] при борьбе за среду уменьшаются, что приводит к меньшему потреблению эфирного времени [airtime]. Наиболее распространенный метод агрегации кадров называется *агрегированный блок данных протокола MAC* [aggregate MAC protocol data unit (A-MPDU)]. Несколько MPDUs могут быть агрегированы в одну передачу. A-MPDU состоит из нескольких MPDUs и присоединены к заголовку PHY.

До 802.11ax, все индивидуальные MPDUs должны были иметь одну и ту же категорию доступа QoS 802.11e, когда использовалась агрегация кадров A-MPDU. Голосовые MPDUs не могли смешиваться с Негарантированными [Best Effort] или Видео [Video] MPDUs внутри одного и того же агрегированного кадра.

Как показано на Рисунке 19.32, Wi-Fi 6 представил *агрегированный блок данных протокола MAC с множеством идентификаторов трафика* [multi-traffic identifier aggregated MAC protocol data unit (multi-TID AMPDU)], который позволяет осуществлять агрегацию кадров от множества идентификаторов трафика [multiple traffic identifiers (TIDs)], от той же самой или другой категории доступа QoS. Возможность смешивать MPDUs разных классов QoS трафика позволяют Wi-Fi 6 агрегировать более эффективно, уменьшая накладные расходы [overhead] и таким образом увеличивая пропускную способность, и следовательно общую сетевую эффективность.

**РИСУНОК 19.32** Multi-TID AMPDU



## Ключевые Вопросы Wi-Fi 6

В этом разделе мы обсуждаем несколько наиболее часто задаваемых вопросов, задаваемых относительно Wi-Fi 6 и технологии 802.11ax.

### Клиенты

К удивлению, нас часто спрашивают, “Будут ли какие-либо клиенты Wi-Fi 6 8×8:8?” Большинство мобильных клиентских устройств Wi-Fi, таких как смартфоны, будут использовать двухчастотные радиомодули 2×2:2, потому что

радиомодуль 8×8:8 израсходует аккумулятор очень быстро. В будущем, вы можете увидеть несколько клиентских радиомодулей Wi-Fi 6 4×4:4 в ноутбуках высшего класса. Все основные производители чипсетов, такие как Broadcom, Qualcomm, и Intel, производят радиомодули 2×2:2 Wi-Fi 6, которые найдут свое место в смартфонах, планшетах и ноутбуках. Samsung выпустил Galaxy S10, первый смартфон Wi-Fi 6, на рынок в Феврале 2019 года. Apple iPhone, представленный в Сентябре 2019, также использовал радиомодуль Wi-Fi 6. Все отраслевые аналитики согласны с тем, что рост технологии Wi-Fi 6 будет быстрым и бешеным. Например, несколько исследовательских фирм прогнозируют, что 1 миллиард чипсетов Wi-Fi 6 будет поставляться ежегодно к 2022 году.

Другой большой вопрос, который нам задают все время - “Будет ли какая-либо выгода по производительности для устаревших клиентов, когда будут развернуты ТД Wi-Fi 6?” Ответ и да, и нет. Сначала плохая новость: Устаревшие клиенты 802.11n/ac не поддерживают механизмы 802.11ax, такие как OFDMA. Следовательно, устаревшие клиенты продолжат использовать однопользовательскую связь при подключении к ТД Wi-Fi 6. Клиентам 802.11ax нужны все преимущества возможностей 802.11 высокой эффективности, таких как многопользовательский OFDMA. Однако, есть и хорошая новость для устаревших клиентов по двум причинам:

- **Оборудование ТД [AP hardware]:** Хотя не будет никаких улучшений на Физическом уровне (PHY) для устаревших клиентов, улучшение производительности будет за счет новых способностей оборудования новых ТД Wi-Fi 6, таких как более мощный CPU и лучшее управление памятью.
- **Доступность эфирного времени [Airtime availability]:** По мере появления большего количества клиентов Wi-Fi 6 в парке клиентских устройств, улучшения эффективности получаемые клиентскими устройствами Wi-Fi 6 будут освобождать ценное эфирное время для устаревших клиентов, улучшая таким образом общую эффективность беспроводной сети.

## МультиГигабитный Ethernet

“Будет ли необходим МультиГигабитный Ethernet?” С каждым новым поколением технологий Wi-Fi и большими скоростями передачи данных заявляются различные полосы в отношении проводного канала подключения между ТД и коммутатором доступа. Так как скорости передачи данных Wi-Fi радикально выросли, то вызывает обеспокоенность, что стандартный 1 Гбит/с проводной канал подключения станет узким местом. Взглянем на это с исторической точки зрения:

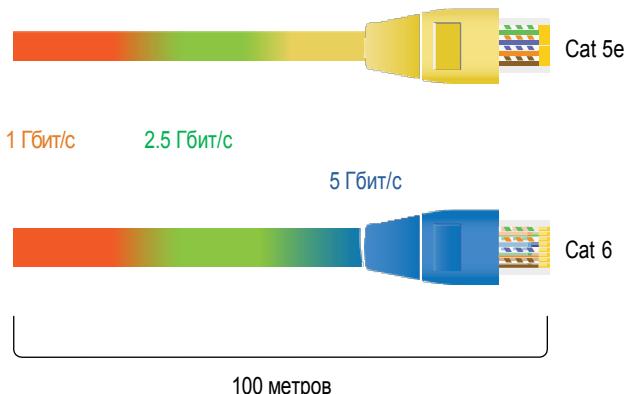
- **802.11n:** В 2009 годы были сделаны заявления, что мы движемся к необходимости агрегирования Gigabit Ethernet (GbE) портов двумя кабелями, когда дебютировал 802.11n. Не произошло.
- **802.11ac:** В 2013 году были сделаны заявления, что мы движемся к необходимости агрегирования GbE портов двумя кабелями, когда появился 802.11ac. Не случилось.
- **802.11ac-Wave 2:** Когда второе поколение чипсетов 802.11ac дебютировало в 2016 году, несколько производителей корпоративных коммутаторов сделали заявления о том, что всем нужно обновить свои коммутаторы для поддержки 2,5 GbE каналов подключения по технологии 802.3bz Multi-Gig Ethernet. Не произошло.

До Wi-Fi 6 (802.11ax), единственный раз когда 1 Гбит/с канала подключения было не достаточно – это в лабораторной тестовой среде или очень уникальном крайнем случае. Узкое место в полосе почти никогда не происходило на уровне доступа. Однако, узкое место по полосе определенно может произойти на проводной сети из-за слабого дизайна проводной сети. Номер один в узких местах по полосе – это

обычно канал подключения к распределенной сети [WAN uplink] из удаленного места. Но можно с уверенностью сказать, что Wi-Fi всегда будут винить первым, несмотря на недостаточную полосу распределенной сети [WAN].

Как показано на Рисунке 19.33, стандарт 802.3bz (также называемый Multi-Gig Ethernet) определяет возможности полосы до 2.5 Гбит/с и 5 Гбит/с по медным кабелям CAT5e и CAT6. Даже возможна полоса в 10 Гбит/с, но она требует повышения класса кабеля до CAT6a или CAT7. Корпоративные производители теперь активно проталкивают продажи коммутаторов доступа, которые поддерживают эти МультиГигабитные скорости.

**РИСУНОК 19.33** Multi-Gig Ethernet—802.3bz



Итак, один вопрос, “Нужны ли будут 2.5 Гбит/с Ethernet порты для точек доступа Wi-Fi 6?” Весь смысл Wi-Fi 6 (802.11ax) в лучшей спектральной эффективности и уменьшения в потреблении эфирного времени. Логика подсказывает, что если Wi-Fi стал более эффективным, пользовательский трафик, генерируемый двухчастотной ТД Wi-Fi 6, может потенциально превысить 1 Гбит/с. Страх в том, что стандартный проводной Gigabit Ethernet порт подключения может быть узким местом, и следовательно понадобится 2.5 Гбит/с порт подключения. В качестве предусмотрительной меры, ТД Wi-Fi 6 производителей БЛВС включают, по крайней мере один 802.3bz Multi-Gig Ethernet порт, поддерживающий 2.5 или 5 Гбит/с проводной канал подключения. Думайте об этом как о заделе на будущее.

В реальном мире, мы вероятно пока еще не превысим 1 Гбит/с еще некоторое время по следующим двум причинам:

- **Парк клиентов Wi-Fi 6 [Wi-Fi 6 client population]:** Несмотря на то, что производители чипсетов агрессивно делают доступными клиентские радиомодули Wi-Fi 6 в тоже самое время, что и радиомодули ТД, потребуется некоторое время прежде чем в основной массе парка корпоративных клиентов будут преобладать Wi-Fi 6 клиенты.
- **Устаревшие клиенты тянут нас вниз:** Wi-Fi 6 требует обратную совместимость с 802.11/a/b/g/n/ac, что означает, что должны использоваться механизмы защиты RTS/CTS. RTS/CTS создает дополнительную служебную информацию [overhead] и потребляет эфирное время [airtime].

Итак, должны ли заказчики обновлять свои коммутаторы, чтобы поддерживать МультиГигабитные возможности? Как мы уже обсуждали, прошлые мрачные и фатальные предсказания об узких местах уровня доступа не сбылись.

Хотя, исторически, канала подключения в 1 Гбит/с более чем достаточно, мы собираемся предсказать, что, по крайней мере, каналы подключения в 2,5 Гбит/с, очевидно, будут нужны. В будущем, по мере роста парка Wi-Fi 6 клиентов, и по мере добавления производителями БЛВС трех-полосных радиомодулей в свои ТД, канала подключения в 1 Гбит/с больше может быть не достаточно. Любое заявление производителей, что нужны будут каналы подключения [uplink] в 10 Гбит/с являются фантазией.

## Питание через Ethernet [Power over Ethernet]

Вероятно намного более важный разговор о взаимосвязи между коммутаторами и ТД Wi-Fi 6 - это требования по Питанию через Ethernet [Power over Ethernet (PoE)]. “Будут ли ТД Wi-Fi 6 работать со стандартным 802.3af PoE?” Во многих случаях, производители корпоративных Wi-Fi будут добавлять больше радиоцепей в свои точки доступа Wi-Fi 6. Многие ТД Wi-Fi 6 будут двух диапазонные ТД 4×4:4, и будут даже ТД 8×8:8. ТД Wi-Fi 6 также будут требовать намного больше вычислительной мощности, чем предыдущие поколения корпоративных ТД. Дополнительные радио цепи и вычислительные возможности будут требовать больше энергии. 15.4 ватта (Вт), предоставляемые на порт по стандарту 802.11af PoE, будет не достаточно для ТД 4×4:4, и следовательно будет нужна мощность 802.3at (PoE Plus). Коммутатор с поддержкой PoE плюс может подать до 30 ватт мощности на Ethernet порт. Порты с питанием по PoE Plus для ТД 4×4:4 должны рассматриваться как стандартное требование.

Если у предприятия нет коммутаторов с поддержкой PoE Plus, то они должны произвести замену на новые с поддержкой PoE Plus, если они собираются разворачивать ТД 4×4:4 802.11ax. Есть хороший шанс, что у многих предприятий уже есть коммутаторы с поддержкой PoE Plus. Но есть ли у коммутаторов достаточно большой бюджет мощности для замены 1:1 с ТД 4×4:4? Что нас волнует, так это то, что у многих предприятий внезапно будет превышен общий бюджет мощности существующих коммутаторов. Производители корпоративного Wi-Fi обычно получают звонки в тех. поддержку от заказчиков, жалующихся, что все ТД внезапно случайным образом начали перезагружаться. В большинстве случаев, корень причины перезагрузки ТД случайным образом в том, что бюджет мощности коммутатора превышен. Очень часто, если ТД не хватает мощности, которая ей нужна, то ТД перезагружается и пробует снова.

Следует следить за бюджетом мощности коммутатора или нескольких коммутаторов, чтобы гарантировать, что все устройства могут получать питание. Информацию об активном бюджете мощности можно обычно посмотреть или в командной строке или графическом интерфейсе (GUI) коммутатора, или мониторить системой сетевого управления (NMS). Модернизация до ТД 4×4:4 как минимум потребует перерасчета бюджета мощности PoE. По мере того как производители БЛВС добавляют больше радиоцепей, двух диапазонные радиомодули, и даже, фактически, трех диапазонные радиомодули, управление бюджетом мощности PoE будет иметь еще важное значение при развитии.

Некоторые производители БЛВС продают ТД 8×8:8 и требования к мощности для PoE еще более серьёзные. В некоторых случаях, эти ТД 8×8:8 требуют 31 или более ватт мощности, что означает, что даже мощности PoE Plus будет не достаточно. Хотя некоторые из ТД 8×8:8 APs могут быть питаны по 802.11at (PoE Plus), существует функционал некоторого рода понижения функциональных возможностей, например отключение USB, радиомодулей BLE, и так далее.

ТД 802.11ax 2×2:2 APs вошли на рынок, и в большинстве случаев, стандартного PoE 14,4 ватта будет не достаточно для питания этих ТД.

## 4x4:4 или 8x8:8

Вероятно, вопрос, который нам задают наиболее часто - это "Что лучше? ТД 8x8:8 или ТД 4x4:4?" Несколько производителей БЛВС продают ТД Wi-Fi 6, у которых есть радиомодуль 2,4 ГГц 4x4:4 и радиомодуль 5 ГГц 8x8:8. Эти производители БЛВС конечно штампуют маркетинговые презентации для 8x8:8. Восемь должно быть лучше, чем четыре—верно?

Теоретически, ТД 8x8:8 может модулировать данные по всем восьми радиоцепям для одного клиента, что в результате приведет к существенно более высокой скорости передачи данных. Проблема в том, что никогда не будет мобильных клиентских устройств 8x8:8 из-за расхода аккумуляторной батареи. Как показано на Рисунке 19.34, мы живем в реальном мире, где основная масса клиентских Wi-Fi устройств - это 2x2:2. И в зависимости от существующих условий, клиенты могут понижать класс до связи 1x1:1.

**РИСУНОК 19.34** Возможности клиентов 2x2:2 и рабочая функциональность



В режиме реального времени и  
Исторической перспективе

Итак, основное преимущество ТД 8x8:8 над ТД 4x4:4 это функциональность MU-MIMO. ТД 8x8:8 может модулировать по два независимых потока данных для каждого из четырех Wi-Fi 6 клиентов 2x2:2, которые поддерживают MU-MIMO в нисходящем канале. Также, ТД 8x8:8 может передавать в нисходящем канале по одному уникальному модулированному потоку данных каждому из восьми Wi-Fi 6 клиентов одновременно. Хотя это звучит хорошо в теории, мы возвращаемся обратно к нашему обсуждению MU-MIMO ранее в этой главе. MU-MIMO требует пространственного разнесения. Даже, если все Wi-Fi 6 клиенты поддерживают MU-MIMO, основная часть современных корпоративных установок Wi-Fi включает высокую плотность пользователей и устройств, что является не идеальным для условий MU-MIMO.

Приемная чувствительность относится к уровню мощности радиосигнала, требуемого для успешного приема радиомодулем приемника. Увеличат ли больше радиоцепей в ТД 8x8:8 приемную чувствительность? Да, если ТД имеет больше принимающих радиомодулей и антенн, чувствительность будет лучше. 8x8:8 может потенциально добавить 3dB приемной чувствительности. Однако, это также создает потенциальный недостаток. Увеличение приемной чувствительности от восьми радиоцепей вероятнее всего

увеличит вероятность одноканальной интерференции [co-channel interference (CCI)] от клиентов, которые принадлежат другим BSSs. Хотя возможности Wi-Fi 6 - цвет BSS и пространственное разнесение могут компенсировать интерференцию OBSS, реальная функциональность возможностей цвета BSS в радиомодулях Wi-Fi 6 не ожидается еще долгое время.

Усиление приемной чувствительности может также увеличить скорость на большой дистанции, что означает, что большие скорости передачи данных могут быть использованы на большем расстоянии. Однако, в большинстве случаев, скорость на большем расстоянии является устаревшей концепцией для Wi-Fi внутри помещений. Из-за высокой плотности клиентов на предприятиях, большинство Wi-Fi сетей проектируются для роуминга, емкости, и уменьшенного потребления эфирного времени. Редко корпоративные БЛВС внутри помещений проектируются с целью работы на больших расстояниях. Стандартное проектирование БЛВС для принимаемого сигнала в  $-70$  дБм уже приводит к тому, что клиенты используют свои возможности по высоким скоростям передачи данных.

ТД  $8\times8:8$  более дорогие и также больше расходуют бюджет мощности PoE. Хотя, в теории усиление MU-MIMO звучит привлекательно, реальность такова, что в большинстве корпоративных установок в помещениях ТД  $8\times8:8$  предлагает не намного больше преимуществ по сравнению с менее дорогой ТД Wi-Fi 6  $4\times4:4$ .

И отгадайте что? Все основные производители БЛВС сейчас продают двухдиапазонные ТД  $2\times2:2$  802.11ax. ТД  $2\times2:2$  в действительности достаточно популярны из-за низкой стоимости. И точки доступа Wi-Fi 6  $2\times2:2$  могут все еще предлагать большую часть преимуществ 802.11ax, включая OFDMA, TWT, 1024-QAM, и многое другое. Независимо от числа радиоцепей, и независимо от числа потоков, все ТД Wi-Fi будут поддерживать одно и тоже количество OFDMA клиентов во время возможности передачи (TXOP).

## Каналы 80 МГц и 160 МГц

802.11ac представил возможности организации 80 МГц и даже 160 МГц каналов в полосе 5 ГГц. Эти большие каналы создаются путем объединения вместе нескольких 20 МГц каналов. Несмотря на то, что 80 МГц и 160 МГц каналы доступны для радиомодулей 802.11ac, их не следует использовать в корпоративной среде. Применение каналов 80 МГц и 160 МГц не масштабируется в корпоративной БЛВС, потому что не достаточно частотного пространства и будет гарантированно происходить одноканальная интерференция [co-channel interference (CCI)]. Объединение каналов также имеет негативный эффект на отношение сигнал-шум [signal-to-noise ratio (SNR)]. Уровни производительности значительно падают, если 80 МГц каналы развернуты на нескольких ТД в любой корпоративной среде.

Еще один вопрос, который часто нам задают - это “Будет ли 80 МГц канал полезен на предприятиях с радиомодулями Wi-Fi 6?” В теории, адаптивные пороги CCA Wi-Fi 6, используемые вместе с цветом BSS, имеют потенциал в минимизации интерференции OBSS. Это сделает развертывание 80 МГц каналов на предприятиях реалистичным с использованием текущего доступного 5 ГГц частотного спектра. Как говорилось ранее в этой главе, хотя цвет BSS и возможности пространственного переиспользования в Wi-Fi 6 могут компенсировать интерференцию OBSS, реальная функциональность возможностей цвета BSS в радиомодулях Wi-Fi 6 еще не ожидается долгое время. В действительности, развертывание 80 МГц и 160 МГц каналов на предприятии не масштабируемо, пока 6 ГГц нелицензируемый спектр не станет доступным.

Тем временем, переиспользование каналов 802.11ax 20 МГц и 40 МГц будет оставаться общепринятой стратегией проектирования на предприятиях. Модели переиспользования 40 МГц каналов могут быть эффективны в

полосе 5 ГГц с хорошим передовым опытом проектирования, упомянутых в Главе 13. Помните, что ТД 802.11ax могут использовать технологию OFDMA для одновременной многопользовательской связи в 40 МГц канале. Например, ТД может синхронизировать передачи в нисходящем и восходящем канале с четырьмя Wi-Fi 6 клиентами, каждому из которых присвоены ресурсные блоки из 106 тонов частотного пространства в 40 МГц канале.

Как было упомянуто в Главе 13, на текущий момент существует много спекуляций о том, что новые правила *спектральной плотности мощности* [*power spectral density (PSD)*] будут компенсировать подъем на 3 дБ в уровне шума при объединении каналов в полосе частот 6 ГГц. В результате, 80 МГц каналы на предприятии могут быть применимы в 6 ГГц. Держите в уме, что 6 ГГц Wi-Fi еще не тестировался в полях; следовательно, остается только смотреть станут ли модели переиспользования 80 МГц каналов на предприятиях преобладающими.

## СЕРТИФИЦИРОВАННЫЙ Wi-Fi 6

Wi-Fi Альянс начал сертификацию по технологии 802.11ax в Августе 2019 года с новой сертификацией с названием СЕРТИФИЦИРОВАННЫЙ Wi-Fi 6 [Wi-Fi CERTIFIED 6]. Так как существует очень много улучшений в 802.11ax, нам бы понадобилось еще страниц 10, чтобы обсудить какие характеристики являются обязательными для ТД или клиентов, чтобы удовлетворять требованиям сертификации Wi-Fi 6. Поэтому вместо этого, мы выделим некоторые главные характеристики Wi-Fi 6.

Наиболее значимая технология для Wi-Fi 6 - это OFDMA. Wi-Fi Альянс требует обязательную поддержку OFDMA и для нисходящего канала [downlink], и для восходящего канала [uplink]. ТД Wi-Fi 6 должна уметь делить 20 МГц канал на четыре ресурсных блока. Поддержка для MU-MIMO в нисходящем канале [downlink] также обязательна для сертифицированных радиомодулей Wi-Fi 6. MU-MIMO в восходящем канале может поддерживаться в будущих поколениях, но поддержка будет опциональной.

Обязательная поддержка требуется для 20 МГц, 40 МГц, и 80 МГц каналов.

Поддержка для 160 МГц каналов опциональна. ТД Wi-Fi 6 должны также поддерживать работу только-20 МГц станций, когда ТД использует каналы больше чем 20 МГц.

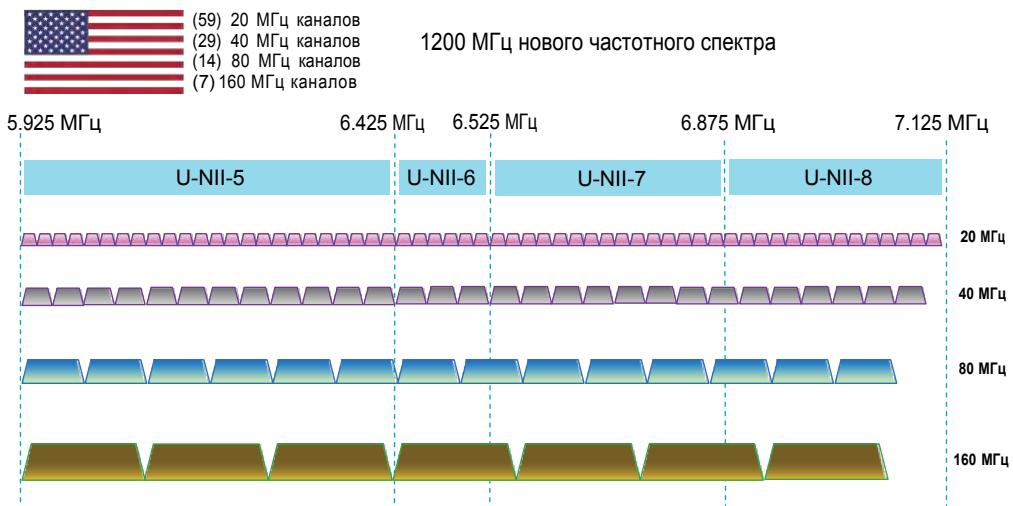
Wi-Fi 6 также представил две новых схемы модуляции и кодирования [modulation and coding schemes (MCSS)], которые используют модуляцию 1024-QAM: MCS-10 и MCS-11, обе являются опциональными для управления питанием 802.11ax. Поддержка индивидуальных TWT является обязательной для ТД, но опциональной для клиентов. Поддержка отчетов о статусе буфера для возможностей QoS является обязательной для Wi-Fi 6 клиентов. Поддержка для некоторых аспектов цвета BSS и работы пространственного переиспользования является обязательной, но на эффективность применения в реальном мире надо еще посмотреть.

Технология Wi-Fi 6 будет работать и в 2.4ГГц и в 5 ГГц полосах частот. Требуется обратная совместимость с 802.11a/b/g/n/ac, и нужны механизмы защиты RTS/CTS. К моменту публикации этой книги Wi-Fi Альянс начал сертификацию радиомодулей 802.11ax для полосы частот 6 ГГц. Wi-Fi Альянс анонсировал Wi-Fi 6E (расширение) программы СЕРТИФИЦИРОВАННЫЙ Wi-Fi 6 [Wi-Fi CERTIFIED 6] в полосе частот 6 ГГц.

Как показано на Рисунке 19.35, Федеральная Комиссия по Связи США [U.S. Federal Communications Commission (FCC)] сделала доступным все 1200 МГц 6 ГГц полосы для нелицензионного использования, и технология 802.11ax будет сертифицироваться как Wi-Fi 6E с 2021 года. Ключевая разница использования 6 ГГц полосы частот для

технологии 802.11ax в том, что не нужна обратная совместимость. Поскольку радиомодули 802.11a/b/g/n/ac работают в 2.4 ГГц или 5 ГГц полосе, и не работают в полосе 6 ГГц, то не нужны механизмы защиты RTS/CTS. Полоса частот 6 ГГц будет "чистой" полосой 802.11ax для Wi-Fi связи.

**РИСУНОК 19.35** Полоса частот 6 ГГц



## ИТОГО

Эта глава сфокусирована на всех улучшениях PHY и MAC, определенных для технологии 802.11ax. Цель 802.11ax в более лучшем и более эффективном управлении трафиком 802.11; таким образом техническое название 802.11ax - это высокая эффективность [high efficiency (HE)]. Большинство отраслевых экспертов верят, что OFDMA наиболее важная технология, которую предлагает 802.11ax. OFDMA обеспечивает более эффективное использование доступного частотного пространства. Дополнительно, впервые, точка доступа будет иметь возможность координировать передачи в восходящем канале [uplink] от клиентских устройств. Синхронизированная связь в восходящем канале определена и для MU-OFDMA и для MU-MIMO. 802.11ax также предоставляет улучшения по экономии заряда батареи для IoT устройств с целевым временем пробуждения [target wake times (TWTs)]. Цвет BSS совместно с работой пространственного переиспользования имеет потенциал по решению вопроса с накладными расходами [overhead] при борьбе за среду из-за перекрывающегося базового состава сервиса [overlapping basic service set] (OBSS).

Важно понимать, что технология 802.11ax все еще относительно новая и тестируется в полях в реальных установках. По мере роста парка Wi-Fi 6 клиентов, улучшения эффективности 802.11ax будут становиться все более очевидными. Введение 6 ГГц полосы частот также поднимет технологию 802.11ax. Неважно, 802.11ax или любая новая технология Wi-Fi не исправит плохой дизайн. Надлежащее проектирование БЛВС и контрольное обследование всегда является критичным.

# Контрольные Вопросы

1. Какое максимальное число ресурсных блоков, которое может быть использовано для 20 МГц OFDMA канала?
  - A. 2
  - B. 4
  - C. 9
  - D. 26
  - E. 52
2. Какой тип кадра 802.11 требуется для связи для восходящего канала [uplink] MU-MIMO или восходящего канала [uplink] MU-OFDMA?
  - A. Триггерный [Trigger]
  - B. Зондирующий [Probe]
  - C. Подтверждения [ACK]
  - D. Маяк [Beacon]
  - E. Данных [Data]
3. Какая технология 802.11ax определяет новые возможности экономии энергии, которые могут быть выгодны для IoT устройств?
  - A. Отчет о статусе буфера [Buffer status report]
  - B. Целевое время пробуждения [Target wake time]
  - C. Цвет БСС [BSS color]
  - D. Защитный интервал [Guard interval]
  - E. Длинное время символа [Long symbol time]
4. Какая технология 802.11ax имеет потенциал по уменьшению одноканальной интерференции [co-channel interference (CCI)]? (Выберите все, что применимо.)
  - A. Отчет о статусе буфера [Buffer status report]
  - B. Целевое время пробуждения [Target wake time]
  - C. Цвет БСС [BSS color]
  - D. Защитный интервал [Guard interval]
  - E. Длинное время символа [Long symbol time]
  - F. Работа пространственного переиспользования [Spatial reuse operation]
5. Какая технология 802.11ax приведет к более высоким скоростям передачи данных, а не к улучшенной эффективности?
  - A. OFDMA
  - B. TWT

- C. 1024-QAM
  - D. Цвет BSS [BSS color]
  - E. SRO
6. Какой минимальный размер ресурсного блока по-умолчанию, если радиомодулем 802.11 ax используется модуляция 1024-QAM?
- A. 26 тонов
  - B. 52 тона
  - C. 106 тонов
  - D. 242 тона
  - E. 484 тона
7. Какая технология 802.11ax предоставляет многопользовательскую связь?
- A. OFDM
  - B. OFDMA
  - C. MIMO
  - D. SU-MIMO
  - E. MU-MIMO
  - F. TWT
  - G. SRO
8. Сколько поднесущих (тонов) в 20 МГц OFDMA канале?
- A. 52
  - B. 64
  - C. 78
  - D. 256
  - E. 312
9. Какая технология 802.11ax позволяет смешивать данные разных категорий доступа QoS при агрегировании кадров 802.11?
- A. OFDMA
  - B. Multi-TID AMPDU
  - C. MU-MIMO
  - D. TWT
  - E. SRO
10. Какие полосы частот определены для беспроводной связи Высокой Эффективности [High Efficiency (HE)]? (Выберите все, что применимо.)
- A. 1 ГГц
  - B. 2.4 ГГц

- C. 5 ГГц
  - D. 6 ГГц
  - E. 60 ГГц
11. Какая многопользовательская технология считается опциональной для Wi-Fi Альянса? (Выберите все, что применимо.)
- A. OFDMA в нисходящем канале [Downlink OFDMA]
  - B. OFDMA в восходящем канале [Uplink OFDMA]
  - C. MU-MIMO в нисходящем канале [Downlink MU-MIMO]
  - D. MU-MIMO в восходящем канале [Uplink MU-MIMO]
12. Когда применяется DL-OFDMA или UL-OFDMA, в чем цель отправки точкой доступа Wi-Fi 6 многопользовательского кадра запроса-на-отправку [multi-user request-to-send (MU-RTS)]? (Выберите все, что применимо.)
- A. Зарезервировать радио среду [Reserve the RF medium]
  - B. Побороться за радиосреду [Contend for the RF medium]
  - C. Выделение ресурсных блоков [Resource unit allocation]
  - D. Запланированное TWT [Scheduled TWT]
  - E. Отсрочка для Интер-БСС [Intra-BSS deferral]
13. Какие из этих форматов 802.11ax PPDU используется для триггерных кадров?
- A. HE SU
  - B. HE MU
  - C. HE ER SU
  - D. HE TB
14. Какой защитный интервал (GI) 802.11ax предназначен только для связи вне помещений [outdoor communications]?
- A. 0.4 микросекунды
  - B. 0.8 микросекунд
  - C. 1.6 микросекунды
  - D. 3.2 микросекунды
  - E. 6.4 микросекунды
15. MU-MIMO связь идеальна для какой среды Wi-Fi в реальном мире?
- A. Wi-Fi сеть высокой клиентской плотности внутри помещений
  - B. Wi-Fi сеть с активным клиентским роумингом внутри помещений
  - C. Wi-Fi мост точка-точка вне помещений
  - D. Wi-Fi мост точка-многоточка вне помещений
16. Какая способность 802.11ax дает клиенту Wi-Fi 6 способность отказаться от синхронизированной связи в восходящем канале и независимо бороться за радиосреду?
- A. ROM
  - B. TOM

- C. QAM
  - D. TWT
  - E. OBSS
17. Какой тип технологии проводного коммутатора доступа наиболее важно принять в рассмотрение при развертывании Wi-Fi 6 точек доступа  $4\times4:4$  или  $8\times8:8$ ?
- A. STP
  - B. SPB
  - C. AVB
  - D. PoE
  - E. IGMP
18. Какой тип кадра 802.11 используется во время UL-OFDMA клиентами Wi-Fi 6 для сообщения ТД о своих потребностях по передаче?
- A. BSR
  - B. BSRP
  - C. MU-RTS
  - D. MU-BAR
  - E. BQRP
19. Какие ключевые различия и преимущества OFDMA над MU-MIMO в радиомодулях 802.11ax? (Выберите все, что применимо.)
- A. Увеличенная эффективность
  - B. Увеличенная емкость
  - C. Лучше для приложений с высокой полосой
  - D. Лучше для приложений с низкой полосой
  - E. Лучше для небольших пакетов
  - F. Лучше для больших пакетов
20. Информация цвет BSS в 802.11ax сообщается и на уровне PHY и на MAC подуровне. Какое из этих утверждений верно о цвете BSS? (Выберите все, что применимо.)
- A. Первичные идентификаторы цвета BSS – это голубой, красный и желтый.
  - B. Вторичные идентификаторы цвета BSS – это зеленый, оранжевый и фиолетовый.
  - C. Цвет BSS это числовой идентификатор.
  - D. Цвет BSS – это идентификатор базового состава сервиса.
  - E. Цвет BSS – это идентификатор области базового сервиса.

# Глава 20



# Установка БЛВС и Вертикальные Рынки

---

**В ЭТОЙ ГЛАВЕ ВЫ УЗНАЕТЕ О СЛЕДУЮЩЕМ:**

- ✓ Рекомендации по развертыванию типовых поддерживаемых БЛВС приложений и устройств
  - Данные
  - Голос
  - Видео
  - Сервисы определения местоположения реального времени (RTLS)
  - Технология зоны непосредственной близости iBeacon
  - Мобильные устройства
- ✓ Доступ к корпоративным данным и мобильность конечных пользователей
- ✓ Расширение сети на удаленные территории
- ✓ Мосты: соединение здание-здание
- ✓ Беспроводной ISP: последняя миля для передачи данных
- ✓ Небольшой офис/домашний офис (SOHO)
- ✓ Временная офисная сеть
- ✓ Офисы филиалов
- ✓ Wi-Fi удаленного работника
- ✓ Использование в образовании/классах
- ✓ Промышленность: склады и производство
- ✓ Розница
- ✓ Здравоохранение
- ✓ Муниципальные сети



- ✓ Хотспоты: сети с публичным доступом
- ✓ Сети Стадионов
- ✓ Сети на транспорте
- ✓ Сети Правоохранительных Органов
- ✓ Сети Служб Экстренного Реагирования
- ✓ Провайдеры Управляемых Услуг
- ✓ Фиксированная мобильная конвергенция
- ✓ БЛВС и здоровье
- ✓ Интернет Вещей
- ✓ Производители БЛВС



В этой главе вы узнаете о средах, где обычно устанавливаются беспроводные сети. Мы рассмотрим за и против беспроводной связи в различных вертикальных рынках БЛВС вместе с рассматриваемым местом установки.

Наконец, мы обсудим основных коммерческих производителей БЛВС и дадим ссылки на их веб сайты.

## Рекомендации по Развертыванию Типовых Поддерживаемых БЛВС Приложений и Устройств

По мере увеличения беспроводных сетей, многочисленные приложения и устройства получили преимущества, и вместе с этим эти приложения и устройства помогли увеличить рост использования беспроводных сетей. Хотя такие приложения, как данные и видео получили преимущества благодаря гибкости и мобильности, которые предоставляются им беспроводной связью, они не являются приложениями присущими только беспроводной связи. Голос, сервисы определения местоположения в реальном времени (RTLS) и сетевой доступ с помощью мобильных устройств являются тремя применениями, которые в своей основе зависят от БЛВС, и продолжат расширять использование БЛВС. Не важно какое из этих приложений вы внедряете на своей сети, вам нужно будет учесть определенные факторы при планировании, проектировании и поддержки вашей БЛВС. Следующие разделы фокусируются на обсуждении типовых поддерживаемых устройств и приложений БЛВС.

### Данные

При обсуждении приложений, ориентированных на данные, первое что приходит на ум - это электронная почта и просмотр веб-страниц. При планировании сетевого трафика по любому типу сети, беспроводной или проводной, вам сначала нужно посмотреть на протоколы, которые будут применены. Протоколы - это способы или методы связи, используемые для связи между устройствами сети. Протоколы могут быть хорошо спроектированы на основе задокументированных стандартов или они могут быть проприетарными, использующими уникальные способы связи. Приложения, ориентированные на данные, часто базируются на хорошо известных протоколах и, следовательно, обычно с ними просто работать, потому что уже существует большая масса знаний о том, как они работают.

Один из наиболее важных аспектов проектирования сети для работы приложений, ориентированных на данные, - это гарантировать, что проект сети способен обработать то количество данных, которое будет передано по сети .

Большинство приложений данных прощают небольшие сетевые задержки, но могут возникнуть проблемы, если не достаточно доступной полосы для данных. Анализируйте требования к данным от ваших пользователей и устройств, и надлежащим образом проектируйте БЛВС, чтобы удовлетворять потребностям. Планирование емкости обсуждается более детально в Главе 13 "Концепции Проектирования БЛВС".

## Голос

При проектировании БЛВС для поддержки голосовой связи, держите в уме, что в отличие от связи для данных, голосовая связь не терпима к сетевым задержкам, сбросу пакетов, или нестабильного соединения. Проектирование БЛВС для поддержки голосовой связи может также быть серьезной задачей, потому что существует очень много различий в том, как производители внедряют свои голосовые продукты. У каждого производителя есть уникальные руководства по проектированию голосовых приложений. Это верно не только для производителей голосовых трубок или программных приложений, но и для производителей инфраструктуры. Поэтому, важно понимать передовой опыт по установке вашей голосовой системы.

Голосовые устройства - это обычно ручные устройства, которые не передают так много мощности, как ноутбуки. Поскольку беспроводные устройства требуют большую мощность батареи, чтобы передавать сильный сигнал, мощность передачи VoWiFi телефонов обычно намного меньше, чем у других устройств, чтобы увеличить длительность батареи.

## Видео

Передача видео обычно сложнее, чем голоса. В дополнении к нескольким потокам данных для видео и голоса, видео часто включает потоки для установки и разрыва соединения. До тех пор, пока вы не используете БЛВС для видеоконференции в реальном времени, видео, скорее всего, может быть на втором плане, по сравнению со звуком. В большинстве случаев, видео имеет большую терпимость к потерям, чем голос. Прерывистый звук во время видеоконференции вероятно будет более деструктивен, заставляя участников просить говорящего повторить то, что было сказано, в то время как, если звук чистый, а видео прерывисто, то говорящего скорее всего поймут с первого раза.

В отношении передачи видео важно идентифицировать тип видео, которое передается, и функцию или назначение этой передачи. Если вы спросите среднестатистического пользователя компьютера о передачи видео, он вероятно подумает о потоковом видео - фильме, телевизионном шоу, или забавных видео клипах, загруженных пользователем, который может быть, как стационарным, так и мобильным. Если вы спросите руководителя о передаче видео, он вероятно подумает о видео как о части видеоконференции или вебинара, и пользователь вероятнее всего будет стационарным. Если вы спросите сотрудника компании, обслуживающей здания, или сотрудника охраны о передаче видео, они вероятно подумают о потоковом видео, генерируемым беспроводными камерами наблюдения, которые наиболее вероятно постоянно прикреплены к зданию. В вашей БЛВС может быть любой или все эти типы видеотрафика.

Когда вы идентифицировали тип видео, который будет использоваться в вашей БЛВС, вы можете начать планировать вашу сеть. Вам нужно оценить систему или программное обеспечение, которое передает беспроводной видео трафик, чтобы определить тип трафика и протоколы вместе с сетевой нагрузкой. Как часть оценки протоколов, вам нужно исследовать использует ли передача видео многонаправленную[multicast] передачу или качество сервиса (QoS).

## Сервисы Определения Местоположения в Реальном Времени

Технологии на основе местоположений привлекли много внимания в проектировании БЛВС. Большинство производителей корпоративных систем БЛВС назойливо рекламируют своего рода возможности определения местоположений в своих продуктах. У кого-то функции встроены, в то время как другие предлагают интеграционные связки со сторонними производителями, которые специализируются на технологиях определения местоположения, и у которых продвинутые программные приложения, относящиеся к конкретной отрасли - вертикальным рынкам.

Отслеживание местоположения расширяется невероятно быстро, так как находится все больше и больше способов применения. Сервисы Определения Местоположения в Реальном Времени [RTLSs] могут быть использованы для определения местоположения или отслеживания людей или устройств в БЛВС. Здравоохранение является одним из самых больших пользователей технологии на основе определения местоположения. Так как поставщики медицинских услуг, такие как больницы, имеют график работы 24/7, и поскольку большая часть инвентаря является общедоступным, RTLSs могут быть чрезвычайно полезны для отслеживания оборудования, которое может быть необходимо в экстренном случае или для определения ближайшего доктора или специалиста.

RTLSs можно использовать для отслеживания радиомодулей 802.11, или специализированных меток 802.11 RFID, которые могут быть прикреплены к не-802.11 инвентарю, чтобы им можно было управлять и отслеживать. Метки могут быть прикреплены к любому устройству, для обеспечения отслеживания, и помочь удержать от кражи. Метки могут также быть прикреплены к сотрудникам, детям в парках развлечений, и больничному персоналу, и пациентам, и так далее. Каждый производитель RTLS уникален и будет способен предоставить вам документы с рекомендациями и успешным применением для установки вашего оборудования RTLS. Хотя решения Wi-Fi RTLS для отслеживания инвентаря все еще имеются в наличии, другие радио технологии, например *ультра-широкая полоса [ultra-wide band (UWB)]*, становятся преобладающими из-за улучшенной точности. Решения RTLS традиционно имеют решения управления поверх [overlay] существующей инфраструктуры; однако, последнее время становится обычным интеграция в облачные решения сетевого управления (NMS) некоторых производителей.

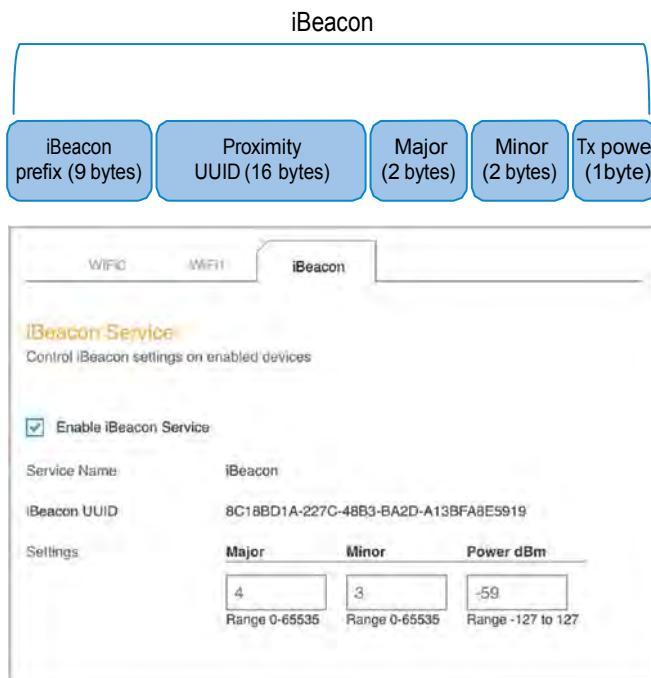
## Технология зоны непосредственной близости iBeacon

Беспроводная технология *Bluetooth Low Energy (BLE)/Bluetooth с Низким Энергопотреблением* сейчас используется во многих новых приложениях в рознице и других коммерческих предприятиях. Хотя Bluetooth - это отличная от Wi-Fi беспроводная технология, многие производители БЛВС интегрируют радиомодули BLE в свои точки доступа или также продают отдельные устройства - BLE передатчики. *iBeacon* - это протокол, разработанный компанией Apple, который использует радиомодули BLE для push-уведомлений внутри помещений в непосредственной близости от определенных мест в розничных предприятиях, стадионах, больницах и других публичных местах проведения мероприятий.

Технология iBeacon основана на зоне непосредственной близости [nearby proximity], а не абсолютно точных координатах местоположения. Радиомодуль BLE в точке доступа передает маяк iBeacon с идентификатором зоны местоположения непосредственной близости [proximity]. Как показано на Рисунке 20.1, идентификатор местоположения зоны непосредственной близости [proximity] состоит из универсального уникального идентификатора [universally unique identifier (UUID)], главного числа, и второстепенного числа. UUID - это 32-символьная шестнадцатеричная строка, которая однозначно определяет организацию, под управлением которой находятся маяки. Например, если сеть магазинов использует маяки в нескольких места, UUID будет названием сети и будет показывать, что все они принадлежат одной и той же организации. UUID включен в полезную нагрузку маяка iBeacon с главным и второстепенными числами, которые обычно показывают определенное место и местоположение внутри этого места, соответственно. UUID находится на самом верху числовой иерархии, с главным [major] и второстепенным [minor] числами, установленными на уровне устройства. В примере на

Рисунок 20.1, значение UUID 8C18BD1A-227C-48B3-BA2D-A13BFA8E5919 может использоваться для идентификации розничной сети Корпорации AKME; значение главного числа [major number] 4 может указывать на магазин AKME, расположенному в Боулдере, Колорадо; а значение второстепенного числа [minor number] может указывать на проход номер 3 между стеллажами в магазине в Боулдере.

**РИСУНОК 20.1** Идентификатор местоположения зоны непосредственной близости [proximity] iBeacon



Организации могут автоматически создать UUID в онлайн генераторе UUID, таком как [www.uuidgenerator.net](http://www.uuidgenerator.net). По факту, большинство UUID сгенерированы именно таким образом, потому что UUID не назначаются и не управляются централизованно. Его 32х-символьная длина делает его безопасным исходя из предположения, что сгенерированный случайным образом UUIDы не создадут дубликаты. Согласно Википедии “для одного из миллиарда шансов дублирования, должно быть сгенерировано 103 триллиона UUID версии 4.”

Маяки iBeacons требуют, чтобы приложение на мобильном устройстве запустило [*trigger*] действие. Запуск происходит, когда смартфон с приемным радиомодулем BLE попадает в зону непосредственной близости [proximity] передатчика iBeacon. Например, iBeacon может запустить push уведомление зоны непосредственной близости такое, как реклама в месте нахождения розничного магазина. Музеи используют технологию чтобы предоставить возможность посетителям пройти самостоятельную экскурсию. Маяки iBeacons могут запускать приложение на мобильных устройствах, чтобы показать интерактивное содержание, когда посетитель находится в непосредственной близости от музеяного экспоната. Как ранее утверждалось, iBeacons используют радиомодули BLE, а не радиомодули 802.11; однако,

многие производители БЛВС теперь предлагают интегрированные и/или работающие поверх решения с технологией iBeacon. Также, пожалуйста, не путайте маяки iBeacons используемые передатчиками BLE с кадрами управления 802.11 типа маяк [beacon], которые передаются Wi-Fi точками доступа. Как упоминалось, iBeacon – это протокол, разработанный Apple для радиомодулей BLE. В 2015 году Google разработал платформу BLE beacon [маяк BLE] с открытым исходным кодом, названную Eddystone. В 2014 году Radius Networks разработала протокол BLE beacon [маяк BLE] с открытым исходным кодом, названным AltBeacon.

## Мобильные Устройства

Сотрудники, от секретарей до директоров, приносят свои собственные устройства с поддержкой 802.11, такие как ноутбуки, планшеты, и смартфоны на работу и ожидают—а во многих случаях требуют—чтобы эти устройства поддерживались в корпоративной сети. Первые устройства, для которых люди требуют доступ – это сотовые телефоны и планшеты, которые могут связываться с помощью радиомодулей 802.11. В отличие от изменений в технологии для предприятий, которые планируются и контролируются ИТ департаментом, поддержка мобильных устройств осуществляется конечным пользователем. Многие организации рассматривают доступ этих устройств как льгота для сотрудников, и оказывают давление на ИТ департаменты для предоставления доступа и поддержки.

Возникает много вопросов по интеграции этих устройств в сеть:

- Убедиться, что устройства способны подключаться к сети с помощью надлежащей аутентификации.
- Обеспечение использования протоколов шифрования с возможностью для этих устройств незаметного роуминга в сети без потери соединения.
- Предоставление сетевого доступа, основанного не только на идентификации пользователя устройства, но также и на типе устройства или других характеристиках устройства или соединения.

Из-за наплыва многочисленных персональных мобильных устройств, таких как смартфоны и планшеты, большинство БЛВС теперь проектируются совершенно по-другому, чтобы удовлетворять потребностям по емкости. В результате, БЛВС внутри помещений редко проектируется строго для больших областей покрытия, а вместо этого проектируются небольшие зоны покрытия, с большим количеством ТД, устанавливаемых для управления требованиями по емкости. Появление таких мобильных устройств стало огромной тенденцией, обычно называемой *принеси свое собственное устройство [bring your own device (BYOD)]*. Это стало таким вопросом, что мы выделили целую главу этой теме, Глава 18 "Устройства Сотрудников (BYOD) и Гостевой Доступ."

## Доступ к Корпоративным Данным и Мобильность Конечных Пользователей

С увеличенной пропускной способностью, предоставленной технологиями 802.11n и теперь 802.11ac, многие организации переходят на эти высокоскоростные беспроводные сети, при этом уменьшая число устройств, подключенных к сети по проводным соединениям—в большинстве случаев

убирая некоторые неиспользуемые или недогруженные проводные коммутаторы. Как упоминалось ранее, еще одно основное влияние, оказывающее давление на организации, для расширения их беспроводных сетей - это быстрое распространение персональных мобильных устройств с Wi-Fi.

Установка проводной сетевой розетки - это дорого, часто стоимость составляет 200 \$ (долларов США) — или даже еще больше — на розетку. По мере того, как компании реорганизуют работников и департаменты, сетевую инфраструктуру обычно тоже нужно менять. Другие территории, такие как склады, конференц-залы, производственные линии, исследовательские лаборатории, и кафетерии, часто являются сложными местами, чтобы эффективно установить проводные сетевые соединения. В этих и других средах установка беспроводных сетей может сэкономить компании деньги и предоставить устойчивый сетевой доступ всем пользователям.

Предоставление непрерывного доступа и доступности в здании стало самым главным за последние несколько лет. С тем, что доступ к компьютеру и данные становятся критичными компонентами работы большинства людей, стало важно для сети быть непрерывно доступной и быть способной предоставить сразу же запрошенную информацию. Путем установки беспроводной сети по зданию или кампусу, компании делают простым для сотрудников возможность собираться и обсуждать или устраивать мозговой штурм, при этом сохраняя доступ к корпоративным данным, электронной почте, и Интернету со своих ноутбуков и мобильных устройств, не зависимо от того где они находятся в здании или кампусе.

Большая тенденция на рынке потребительской электроники стала добавление беспроводного радиомодуля в устройства. Беспроводные адаптеры чрезвычайно маленькие и могут быть просто интегрированы в эти портативные устройства. Подключение к Интернету также позволяет устройствам быть легко обновляемыми, вместе с предоставлением больших возможностей. В дополнение к тенденции подключаемой персональной электроники, устройства продолжают становиться меньше, легче и тоньше. С этим стремлением к более тонким устройствам, Ethernet адAPTERы уступили дорогу беспроводным радиомодулям, или от них полностью отказались в пользу беспроводной связи.

Какая бы ни была причина по установке беспроводной сети, компании должны помнить об ее преимуществах и недостатках. Беспроводная связь предоставляет мобильность, доступность, и удобство, но, если она не спроектирована и не установлена надлежащим образом, ей может не хватать производительности, доступности и пропускной способности. Беспроводная связь является технологией доступа, обеспечивающей подключение станций конечных пользователей. Беспроводная связь редко рассматривается для роли дистрибуции или ядра, кроме моста здание-здание или транзитного канала для взаимосвязности [mesh backhaul]. Даже в этих сценариях, убедитесь, что беспроводной мост будет способен справиться с нагрузкой трафика и потребностями пропускной способности.

## Расширение Сети на Удаленные Территории

Если хорошенько подумать, то расширение сети на удаленные территории было одной из движущих сил домашних беспроводных сетей, которые также помогали двигать спрос на беспроводную связь в корпоративной среде. Так как домовладения подключались к Интернету, и так как все больше домовладений покупали дополнительные компьютеры, то была необходимость подключить все компьютеры в доме к Интернету. Хотя многие люди проводили кабель Ethernet для подключения своих компьютеров,

обычно это было очень дорого, непрактично, из-за доступности, или за пределами технических возможностей среднестатистического домовладельца.

В тоже самое время, беспроводные устройства 802.11 становились более доступны по средствам. Те же самые причины для установки беспроводных сетей дома верны для установки беспроводной связи в офисах, складах и в любой другой среде. Стоимость установки сетевого кабеля для каждого компьютера высока, и во многих средах, протягивание кабеля или оптоволокна является сложным из-за дизайна здания или эстетических ограничений. Когда оборудование беспроводной сети установлено, то требуется намного меньше кабелей, а размещение оборудования часто может быть выполнено без влияния на эстетику здания.

## Мосты: Соединение Здание-Здание

Чтобы обеспечить сетевую связность между двумя зданиями, вы можете проложить подземный кабель или оптоволокно между двумя зданиями, вы можете заплатить за арендованный высокоскоростной канал передачи данных, или можете использовать беспроводной мост здание-здания. Все три решения жизнеспособны, каждый со своими преимуществами и недостатками.

Хотя подключение по меди или оптоволокну между двумя зданиями потенциально даст вам самую высокую пропускную способность, прокладка медных кабелей или оптоволокна между двумя зданиями может быть дорогой. Если здания разделяет большое расстояние или чья-то еще собственность, то это уже может быть не вариант. После прокладки кабеля нет ежемесячных платежей, так как это ваш собственный кабель.

Аренда высокоскоростной линии передачи данных может предоставить гибкость и удобство, но так как это не ваше собственное соединение, вы будете платить ежемесячную плату за услугу. В зависимости от типа услуги, за которую вы платите, вы сможете или не сможете легко увеличить скорость канала связи.

Беспроводной мост здание-здания требует, чтобы между зданиями была чистая линия прямой радиовидимости. После того, как это определено или создано, могут быть установлены антенна и приемопередатчик точка-точка (PtP) или точка-многоточка (PtMP). Установка обычно легко выполняется опытными профессионалами, и нет никаких ежемесячных платежей после установки, так как это ваше собственное оборудование.

В дополнение к соединению двух зданий PtP мостом, три или более зданий могут быть связаны вместе с помощью решения PtMP. В установке PtMP, здание, которое более всех расположено в центре, будет центральной точкой связи, а другие устройства будут связываться прямо с центральным зданием. Это называется конфигурацией *hub and spoke* [ступица и спица] или конфигурацией типа *звезда* [star]. Беспроводные мосты 802.11 обычно устанавливаются для коротких расстояний в 5 ГГц полосе частот U-NII-3. Многие предприятия вместо этого выбирают решение беспроводного моста, который передает на лицензируемых частотах. Компании, такие как Cambium Networks ([www.cambiumnetworks.com](http://www.cambiumnetworks.com)) предлагает и лицензируемое, и нелицензируемое решения по наружным транзитным [backhaul] каналам.



Потенциальная проблема с решением точка-многоточка (PtMP) в том, что центральная точка связи становится единой точкой отказа для всех зданий. Чтобы избежать ситуации с единой точкой отказа и предоставить более высокую пропускную способность передачи данных, не является чем-то необычным установка нескольких мостов точка-многоточка.

## Беспроводной ISP: Последняя Миля для Передачи Данных

Термин *последняя миля [last mile]* часто используется телефонными и кабельными компаниями для обозначения последнего сегмента их сервиса, который подключает домашнего абонента к их сети. Последняя миля услуги часто является самой сложной и дорогой для запуска, потому что в этой точке кабель должен быть проложен индивидуально каждому абоненту. Это особенно верно в сельской местности, где очень мало абонентов и они разделены большими расстояниями. Во многих случаях, даже если абонент подключен, абонент не может получить некоторые услуги, такие как высокоскоростной Интернет, потому что такие услуги, как xDSL имеет ограничение по максимальной длине в 18000 футов (5,7 км) от центрального офиса.

*Беспроводные Интернет сервис провайдеры [Wireless Internet service providers (WISPs)]* предоставляют услуги Интернет через беспроводную сеть. Вместо прямого кабельного подключения каждого абонента, WISP может предоставлять услуги через радиосвязь с центральных передатчиков. WISPs часто используют другие беспроводные технологии, а не 802.11, позволяющие им предоставлять беспроводное покрытие намного больших территорий. Некоторые небольшие города добились успеха в использовании взаимосвязных [mesh] сетей 802.11 в качестве инфраструктуры для WISP. Однако, в общем технология 802.11 не предназначена для масштабирования до размеров, необходимых для развертывания WISP для охвата крупных городов.

Услуга от WISPs не без собственных проблем. Как и любой радиотехнологией, сигнал может ухудшиться или быть поврежденным препятствиями, такими как крыши, горы, деревья, и другие строения. Надлежащее проектирование и профессиональная установка могут гарантировать надлежащим образом работающую систему.

## Небольшой Офис/Домашний Офис

Одна общая тема *небольшого офиса/домашнего офиса [small office/home office (SOHO)]* в том, что описание вашей должности растягивается от уборщицы до ИТ персонала и включает все, что между ними. От собственников небольших предприятий и сотрудников домашних офисов обычно требуется быть самодостаточными, потому что обычно вокруг немного людей, если вообще есть, которые могли бы помочь им. Беспроводная сеть помогла сделать простым для сотрудника SOHO соединения офисных компьютеров и периферийных устройств вместе, а также с Интернетом. Главная задача сети 802.11 SOHO обычно предоставить беспроводной доступ к Интернет шлюзу. Как показано на Рисунке 20.2, многие потребительского класса Wi-Fi маршрутизаторы также имеют несколько Ethernet портов, обеспечивающих как проводной, так и беспроводной доступ в Интернет.

**РИСУНОК 20.2** Беспроводной SOHO маршрутизатор D-Link

Большинство беспроводных маршрутизаторов потребительского класса предоставляют довольно простые инструкции по установке и предлагают приемлемую производительность и безопасность, хотя и меньшую, нежели чем предоставляет корпоративный аналог. В целом они не такие гибкие или богатые характеристиками по сравнению с корпоративными продуктами, но большинству SOHO сред не нужны все дополнительные возможности и характеристики. Что получает потребитель - это пригодное устройство за четверть цены от корпоративного аналога. Доступны десятки устройств для обеспечения домашних работников возможностью по установке и настройке своей сети с подключением в Интернет не тратя целое состояние. Многие беспроводные маршрутизаторы потребительского класса даже имеют возможность предоставления гостевого доступа, позволяя посетителям иметь доступ в Интернет при этом предотвращая их доступ к локальной сети. Последние годы несколько компаний, включая Google, eero, Linksys, Plume, и других, также начали предлагать полное решение домашнего Wi-Fi, которое включает три или более домашних взаимосвязанных [mesh] маршрутизатора БЛВС и приложение для смартфона, которое может управлять устройствами БЛВС. Основной фокус этой книги был в обсуждении БЛВС предприятий. Однако, значительно больший рынок - это Wi-Fi потребительского класса для домашних пользователей, потому что почти у всех есть Wi-Fi дома.

## Временная Офисная Сеть

Мобильные дома или передвижные офисы используются для многих целей—например, как временный офис при строительстве, или после стихийного бедствия, или в качестве класса, чтобы обеспечить незапланированное изменение в количестве студентов. Временные офисы - это просто расширение офисной среды. Эти структуры - это обычно здания на колесах, которые могут быть легко развернуты на короткий или длительный срок по мере необходимости. Так как эти структуры не постоянны, то обычно легко расширить корпоративную или школьную сеть на эти офисы с помощью беспроводной сети.

Беспроводной мост может быть использован для доставки беспроводной сети на мобильный офис. Если нужно, то ТД может затем использоваться для обеспечения беспроводного сетевого доступа нескольким персонам офиса. Путем предоставления сети через беспроводную связь, вы можете уменьшить затраты на прокладку кабелей и установку розеток. Дополнительные пользователи могут подключаться и отключаться от

сети без необходимости каких-либо изменений на сетевой инфраструктуре. Когда временный офис больше не нужен, беспроводное оборудование может быть просто выключено и убрано.

Перевозимые беспроводные сети используются во многих средах, включая военные маневры, оказание помощи во время стихийных бедствий, концертов, блошиных рынках и на объектах строительства. Из-за простоты установки и демонтажа, мобильные беспроводные сети могут быть идеальным сетевым решением.

## Офисы Филиалов

В дополнение к главному корпоративному офису у компаний есть офисы филиалов в удаленных местах. У компании могут быть офисы по всему региону, целой стране, или даже по всему миру. Задача для ИТ персонала в том, как обеспечить бесшовное проводное и беспроводное решение по всем локациям. Распределенное решение, использующее корпоративного класса маршрутизаторы БЛВС в каждом офисе филиала является общепринятым выбором. Филиальные маршрутизаторы БЛВС могут соединить с корпоративной штаб-квартирой по VPN туннелям. Сотрудники в офисах филиалов могут иметь доступ к корпоративным ресурсам через распределенную сеть (WAN) через VPN туннель. Даже более важен тот факт, что корпоративные VLANы, SSID, и безопасность БЛВС может быть расширена на удаленные офисы филиалов.

Сотрудник в офисе филиала подключается к тому же самому SSID, к которому он подключался бы в корпоративной штаб-квартире. Политики проводного и беспроводного сетевого доступа, следовательно, являются плавными, без резких изменений по всей организации. Эти бесшовные политики могут быть расширены на маршрутизаторы БЛВС, точки доступа, и коммутаторы в каждом филиале. Решения с филиальным маршрутизатором обычно применяют IPSec VPN 2ого уровня и используют внутренние возможности DHCP вместе с NAT, чтобы предоставить локальную связность по IP. Внутренний межсетевой экран также может направлять пользовательский трафик в компанию по VPN туннелю или направлять трафик на локальный шлюз филиального маршрутизатора БЛВС.

У большинства компаний нет такой роскоши или нужды, чтобы иметь ИТ персонал в каждом офисе филиала. Следовательно, сервер сетевого управления (NMS) в центральной локации используется для управления и мониторинга всей корпоративной сети.

## Wi-Fi Удаленного Работника

*Удаленный сотрудник [teleworker]* это тот, кто работает из дома за компьютером и связывается со своими коллегами и заказчиками по телефону и через Интернет. С несчастным появлением пандемии COVID-19 компании были вынуждены адаптироваться к предоставлению удаленного доступа к корпоративным ресурсам для сотрудников, которые теперь работают из дома. Большей части удаленных работников нужен быстрый и прямой способ доступа к тем же самым ресурсам, как и корпоративным пользователям, которые продолжают работать в корпоративной штаб-квартире.

Производители БЛВС предлагают эффективное по стоимости решение для удаленных сотрудников для безопасного доступа к корпоративным ресурсам через IPSec VPN 2ого уровня с помощью точки доступа компании. Удаленные ТД корпоративного класса работают как конечные точки VPN 2ого уровня в доме удаленного сотрудника, и могут автоматически поддерживаться через систему сетевого управления (NMS).

Более того, та же самая сеть, которая существует в штаб-квартире, расширяется в дом удаленного сотрудника. IP связность обычно обеспечивается DHCP сервером из корпоративной штаб квартиры.

## Использование в Образовании/Классах

Беспроводная сеть может быть использована для предоставления безопасного и простого способа подключения учеников к школьной сети. Поскольку планировка большинства классов гибкая (без жестко установленной мебели), установка проводных сетевых розеток для каждого ученика невозможна. Так как школьники будут постоянно подключаться и отключаться от сети в начале и конце урока, розетки долго не протянут, даже если бы они были установлены. До беспроводных сетей, в классах, где был проводной Ethernet, обычно все компьютеры стояли на столах вдоль стен, а школьники обычно сидели лицом от инструктора. Беспроводные сети позволяют использовать любую рассадку в классе без риска запутаться или споткнуться о сетевые кабели, растянутые по полу.

Беспроводная сеть также позволяет ученикам подключиться к сети и работать в школьной сети в любом месте здания без заботы о том есть ли поблизости розетка проводной сети или ее уже кто-то использует. В дополнении к гибкости беспроводная сеть может поддержать среду класса, в большинстве школ беспроводная сеть стала необходимостью; компьютерные планшеты быстро стали обычными устройствами на всех уровнях обучения. Эти планшеты полагаются только на беспроводную сеть для доступа в Интернет и локальную вычислительную сеть.

Школы обычно требуют больше точек доступа для покрытия, из-за плотности материалов стен между классами. Большинство стен классов сделаны из шлакоблоков чтобы поглощать шум между классами. Шлакоблоки также значительно поглощают радиосигналы 2,4 ГГц и 5 ГГц. Для того, чтобы обеспечить покрытие в -70 дБм или больше, точка доступа должна быть, как минимум, в каждом классе.

Использование беспроводных мостов также преобладает в кампусных средах. Многие университеты и колледжи используют много типов беспроводных мостов, включая 802.11, чтобы соединить здания по всему кампусу.



### Пример из Реальной Жизни

#### eduroam

Многие университеты высшего образования используют решение аутентификации на основе доменов [realm-based], которое называется **eduroam** (education roaming – институтский роуминг). Технология в eduroam основана на стандарте IEEE 802.1X и иерархии RADIUS-прокси серверов. eduroam – это безопасный, всемирный роуминговый сервис доступа, разработанный для международных исследовательских сообществ и сообществ высшего образования. eduroam позволяет студентам, исследователям, и персоналу участвующих институтов получить подключение к Интернету в кампусе и при посещении других участвующих институтов. Аутентификация пользователей выполняется их домашним институтом, используя те же самые учетные данные, когда они получают доступ к сети локально. В зависимости от локальных политик в посещаемом институте, участники eduroam могут также иметь дополнительные ресурсы в их расположении.

Архитектура для Сетевого Роуминга eduroam определена в RFC 7593. Больше информации о сервисе eduroam можно найти на [www.eduroam.org](http://www.eduroam.org).

# Промышленность: Склад и Производство

Складские и производственные помещения – это две среды, в которых беспроводная сеть используется много лет, даже до того, как был создан стандарт 802.11. Из-за огромного пространства и мобильной природы сотрудников в этих средах, компании видят необходимость в обеспечении мобильного сетевого доступа для своих сотрудников, чтобы они могли более эффективно выполнять свою работу. Складские и производственные среды часто используют беспроводные ручные устройства, такие как сканеры штрихкодов, которые используются для сбора данных и инвентарного учета. Как вы узнали в Главе 13, проектирование БЛВС совершенно другое и часто требует использования направленных антенн.

Большинство сетей 802.11, развернутых и на складских и производственных средах, спроектированы для покрытия, а не для емкости. Ручные устройства обычно не требуют много полосы, но нужны огромные области покрытия для предоставления реальной мобильности. Более ранние установки в производственных и складских средах была технология 802.11 с перестройкой частоты. Беспроводные сети могут предоставить покрытие и мобильность, требуемую в складской среде — и обеспечить это эффективно по стоимости.

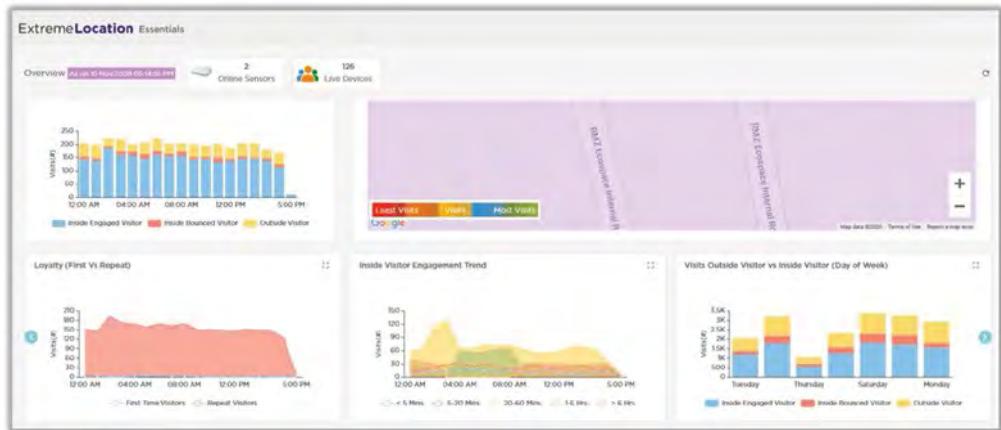
# Розница

Существует четыре ключевых применения беспроводной связи в местах розничной торговли. Первое – это беспроводная сеть, которая предоставляет поддержку, касающуюся работы магазина и розничных транзакций. Второе – это более новое и растущее применение, которое является аналитикой отслеживания розничных покупателей. Третье – это сервис указания на карте местоположения и сервис отслеживания перемещений. Четвертое – это вспомогательный гостевой Wi-Fi с доступом в Интернет, часто необходимы из-за слабого сотового покрытия внутри предприятия розничной торговли.

Среда розничной торговли аналогична многим другим средам других предприятий. Кассовые аппараты, регистраторы времени прихода и ухода, сканеры инвентарного учета, и просто каждое электронное устройство, используемое для работы торговой точки, становятся сетевыми с радиомодулями БЛВС. Подключение этих устройств обеспечивает более быструю и более точную информацию, и улучшает среду розничной торговли для покупателя.

Чтобы больше поддержать и понять заказчика и его поведение, устанавливаются продукты розничной аналитики, чтобы мониторить перемещение заказчика и его поведение. Стратегически размещенные точки доступа или сенсорные устройства слушают кадры зондирующих запросов [probe request] от смартфонов с включенным Wi-Fi. MAC адреса используются для идентификации каждого уникального Wi-Fi устройства, а сила сигнала используется для мониторинга и отслеживания местоположения покупателя. Рисунок 20.3 показывает панель розничной аналитики. Аналитика может определить путь, который прошел покупатель, во время прохода по магазину, и время, проведенное в различных местах магазина. Эта информация может быть использована для идентификации покупательской модели вместе с анализом эффективности дисплеев и рекламы в магазине. Эти решения розничной Wi-Fi аналитики иногда называются как аналитика присутствия [*presence analytics*].

**РИСУНОК 20.3** Розничная аналитика



Как ранее упоминалось, технология iBeacon также часто используется розничными предприятиями для предоставления push уведомлений и анализа тенденций. В дополнение к приложениям розничной технологии непосредственной близости от определенного места [retail proximity location] и анализу тенденций, положению внутри помещения и отображения на карте, стали предоставлять новые сервисы по поддержке покупателей и посетителей. Центры розничной торговли, больницы, гостиницы, метро и музеи (и многие другие типы организаций) могут предоставить пошаговые инструкции посетителям, вместе с рекламными акциями и другими услугами, на основе местоположения. Как пример, навигация по большой больнице может быть запутанной. Мобильное приложение может предоставить пошаговые указания для семьи и друзей, чтобы найти палату пациента. Конференц-центры и гостиницы могут использовать эти технологии, чтобы направлять посетителей в залы для встреч и мероприятий. Специальные события, реклама, или услуги могут быть предложены посетителю по мере того как он направляется через здание.

Еще одна ключевая причина по внедрению беспроводной связи в торговых точках - это предоставление дополнительной связи вместо покрытия сотовой связи. Торговые точки не могут зависеть от того, есть ли у заказчика доступ в Интернет через свою сотовую телефонную сеть. Из-за масштабов и часто плотности продуктов, на телефоне сотовая сеть может быть не доступна или быть ненадежной. Предоставление гостевого Wi-Fi доступа для покупателей может сделать процесс покупок более приятным и удовлетворительным, и вероятно приведет к большим продажам. Глубокое обсуждение доступа к гостевой БЛВС можно найти в Главе 18.

# Здравоохранение

Хотя медицинские учреждения, такие как больницы, клиники и медицинские центры могут казаться сильно отличающимися от других предприятий, у них много тех же самых сетевых потребностей как и у других компаний: доступ к данным и мобильность конечных пользователей. Поставщикам медицинских услуг нужен быстрый, безопасный и точный доступ к данным пациента и больницы или клиники, чтобы они могли реагировать и принимать решения. Беспроводные сети могут предоставить мобильность, давая поставщикам медицинских услуг более быстрый доступ к важным данным путем доставки данных прямо на ручные устройства, которые доктора или медицинские сестры носят с собой. Медицинские карты, используемые для ввода и мониторинга информации о пациенте, часто имеют беспроводное соединение с сестринским постом. Многие компании медицинских устройств, включая Masimo ([www.masimo.com](http://www.masimo.com)), встраивают беспроводные 802.11 адаптеры в свое медицинское оборудование чтобы мониторить и отслеживать жизненные показатели пациента, например: носимая пациентом система мониторинга показана на Рисунке 20.4. Стационарные и мобильные, носимые пациентом медицинские мониторы могут использовать Wi-Fi для безопасной передачи ЭКГ пациента, кровяного давления, дыхания, и других жизненных параметров на сестринский пост.

**РИСУНОК 20.4** Носимый пациентом монитор Masimo Root с Radius-7



VoWiFi - это еще одно типовое использование технологии 802.11 в медицинской среде, предоставляющей мгновенный доступ персоналу, не важно где он находится в здании. Решения RTLS, использующая 802.11 Wi-Fi метки для контроля инвентаря также является обычным делом.

Больницы опираются на многие формы проприетарной и стандартной отраслевой беспроводной связи, которая может иметь потенциал вызывать радиоинтерференцию с беспроводными сетями 802.11. Во многих больницах есть назначенный человек или департамент по управлению спектром, чтобы помочь избежать радиоконфликтов путем отслеживания частот и биомедицинского оборудования, используемого в больнице.

Распределенное медицинское обслуживание также является новой тенденцией. У больниц часто есть много удаленных филиалов. Пункты неотложной медицинской помощи широко распределены и очень часто требуют решение по БЛВС для филиальных офисов.

## Муниципальные Сети

Муниципальные сети получили много внимания за последние годы. Большие и малые города анонсировали свою заинтересованность в предоставлении беспроводного сетевого доступа для своих граждан по всей территории. Многие муниципалитеты рассматривают это как способ предоставления услуги некоторым своим жителям, которые не всегда могут позволить себе доступ в Интернет. Хотя это благая идея, общество часто недооценивает масштаб и стоимость этих проектов, и многие налогоплательщики не хотят, чтобы их налоги тратились на то, что они считают ненужным сервисом. Хотя большинство из этих ранних планов для общегородских муниципальных сетей 802.11 были списаны, существует возросший интерес и успех в развертывании 802.11 в деловых центрах городов и местах с высокой плотностью. Некоторые из них предоставляются муниципалитетами, а другие предоставляются отдельными лицами или группами предприятий.

## Хотспоты: Сети Публичного Доступа

Термином *hotspot* [hotspot] обычно называют бесплатную или платную беспроводную сеть, которая предоставляется как услуга предприятием. Когда люди думают о хотспотах, они обычно ассоциируют их с кафе, книжными магазинами или бизнесом гостеприимства, таким как гостиницы или конференц-центрами. Хотспоты могут эффективно использоваться, чтобы привлечь заказчиков или как расширение сервисов—в случае Интернет провайдеров, предлагающих эти услуги в районах с интенсивным движением. Командировочные и студенты знают, что очень часто рестораны и кафе предоставляют бесплатный доступ в Интернет. Многие из этих заведений получают выгоду от увеличения бизнеса, генерируемого путем предложения хотспота. Бесплатные хотспоты привлекли много внимания к отрасли беспроводной связи 802.11, помогая познакомить больше людей с преимуществами этой технологии.

Другие провайдеры хотспотов испытывают трудности с убеждением людей платить более 40\$ в месяц за абонентскую плату (подписку). Многие аэропорты и сети отелей установили платные хотспоты; однако, существует много провайдеров, каждый из которых предлагает отдельную подписку, которая чаще всего не практична для потребителя.

Большинство провайдеров хотспотов осуществляют аутентификацию с помощью специального типа веб страницы, называемую *перехватывающий портал* [*captive portal*]. Когда пользователь подключается к хотспоту, пользователь должен открыть веб браузер.

Не важно на какую веб страницу пытается зайти пользователь, вместо нее будет показана веб страница входа [login web page], как показано на Рисунке 20.5. Это страница перехватывающего портала [captive portal]. Если хотспот провайдер это платный сервис, то пользователь должен или ввести информацию о своей подписке, если он абонент (подписчик) этой услуги, или информацию своей кредитной карты, если он оплачивает почасовое или посугточное использование. Многие бесплатные хотспоты также используют перехватывающие порталы [captive portals] как способ потребовать от пользователя согласиться с политикой использования, прежде чем ему будет разрешен доступ в Интернет. Если пользователь соглашается с условиями политики, то ему требуется или ввести некоторую базовую информацию или нажать кнопку, подтверждающую его согласие с политикой использования. Многие корпорации также могут использовать перехватывающие порталы [captive portals] для аутентификации гостевых пользователей в своих корпоративных сетях.

**РИСУНОК 20.5** Пример перехватывающего портала

Sign up | Connection plan > Payment/Terms > Authentication

United States Germany France Italy Spain China Japan South Korea

## Welcome to iBAHN - Please Choose a Connection Plan

**PREMIUM INTERNET**

Provides premium high-speed Internet access

**Ideal for:**

- VPN connections
- Downloading large files
- Video and music streaming

24 hours - \$ 12.95

**SPECIAL PROGRAMS**

Choose from one of our Special Programs

Subscription Service

Connect Code

Next Next

By proceeding, you agree to the Terms of Use ([Read](#))

Marriott Rewards ® Gold and Platinum Elite members receive complimentary Internet access as part of their Elite benefits package.  
(Applicable charges will be adjusted prior to departure for these guests.) Please choose your preferred service.

Copyright © 2008 iBAHN. All Rights Reserved.

### Пример из Реальной Жизни

#### Обеспечивает ли Хотспот Безопасность Данных?

Важно помнить, что хотспоты провайдеры (бесплатные или платные) обычно не заботятся о безопасности ваших данных. Бесплатный провайдер обычно предлагает вам доступ в Интернет как способ сподвигнуть вас посетить его место, такое как кафе и купить что-нибудь из того, что они продают. Провайдеры платных хотспотов осуществляют аутентификацию, чтобы убедиться, что вы оплаченный абонент, и после подтверждения этого, они предоставляют вам доступ в Интернет. Кроме редких случаев, ни один из этих хотспот провайдеров не выполняет шифрование данных. Из-за этого, бизнес пользователи часто используют программный VPN клиент, чтобы обеспечить безопасный шифрованный туннель в корпоративную сеть, где бы они не использовали хотспот. Многие компании требуют, чтобы сотрудники использовали VPN во время любого подключения к публичной сети. Проблема в том, что многие потребители и гостевые пользователи недостаточно сообразительны, чтобы знать, как использовать решение VPN при подключении к открытой гостевой БЛВС. В результате, существует свежая тенденция в предоставлении шифрования, а еще лучше безопасной аутентификации для гостевых пользователей БЛВС.

Еще одна растущая тенденция с сетями с публичным доступом – это использование 802.1X/EAP с технологией Хотспот 2.0. Хотспот 2.0 - это техническая спецификация Wi-Fi Альянса, которая поддерживается сертификационной программой Пасспоинт [Passpoint]. Более глубокое обсуждение о шифрованном гостевом доступе и Хотспот 2.0 можно найти в Главе 18.

## Сети Стадионов

Технологически продвинутые фанаты приезжают на спортивные, концертные события и мероприятия на стадионах и аренах, чтобы увеличить свои услуги. Фанаты ожидают и запрашивают полное мультимедийное оснащение при посещении мероприятий, включая доступ к повторам и статистике в реальном времени. С помощью приложения или вебсайта заказ и доставка еды и напитков на свое место улучшает впечатление, позволяя фанатам получать удовольствие от действия вместо того, чтобы стоять в очереди чтобы перекусить. С помощью текстовых сообщений и социальных сетей фанаты ожидают иметь возможность поделиться своими впечатлениями с друзьями или обмениваться впечатлениями с другими посетителями. Теперь на стадионах и спортивных событиях используется технология iBeacon.

Хорошо спроектированная стадионная сеть может позволить месту проведения направить на секции или группы людей целевую рекламу, специальные предложения, или индивидуальные услуги. Предложения или услуги для болельщиков на трибунах вероятно будут отличаться от тех, что предлагаются болельщикам в скайбоксах (vip-ложах). В дополнении к предоставлению беспроводных услуг болельщикам, важно помнить, что стадион – это предприятие и нужна поддержка его собственной инфраструктуры и услуг на мероприятии. Беспроводные сети нужны, чтобы обеспечить работу мероприятия такими услугами, как надежный высокоскоростной доступ в Интернет в местах размещения сотрудников прессы, продажи и проверки билетов и обработки транзакций точек продаж, и охранного видеонаблюдения. Из-за высокой плотности пользователей для мероприятий на стадионе нужно несколько широкополосных и зарезервированных каналов подключения к внешним сетям [WAN uplinks].

## Сети Транспорта

Большинство дискуссий о Wi-Fi сетях на транспорте упоминают три основных режима транспорта: поезда, самолеты, и автомобили. В дополнение к этим трем первичным вариантам транспорта, два других заслуживают внимания: корабли (и круизные корабли и регулярные пассажирские перевозки) и автобусы (которые похожи, но отличаются от автомобилей).

Предоставление Wi-Fi сервиса на любом виде транспорта является простым; просто установите одну или более точек доступа на транспорте. За исключением круизных кораблей и крупных регулярных перевозчиков, большинству из этих видов транспорта требуется не много точек доступа, чтобы обеспечить Wi-Fi покрытие. Первичное использование этих сетей – это предоставление сервисов хотспот для конечных пользователей, чтобы они могли получить доступ в Интернет. Разница между сетью на транспорте и обычным хотспотом в том, что эта сеть постоянно движется, делая необходимым для транспортной сети использовать некоторый тип сервисов с мобильным каналом подключения.

Чтобы обеспечить канал подключения [uplink] для поезда, который привязан к одному и тому же пути следования для каждой поездки, может использоваться технология городской беспроводной сети, такой как спутниковый или сотовый LTE вдоль пути. В других транспортных сетях, для которых путь следования менее ограничен, вероятнее всего способ канала подключения будет через некоторый тип сотового или спутникового сетевого соединения.

Регулярные перевозчики вероятно обеспечивают каналы подключения [uplink] через спутниковый или сотовый LTE, потому что они скорее всего находятся в зоне действия этих сервисов. Для круизных кораблей и перевозчиков, которые идут далеко от берега, обычно используется спутниковый канал.

Многие авиалинии или уже установили, или в процессе установки Wi-Fi на свои самолеты. Wi-Fi сервис на самолете состоит из одной или более точек доступа, подключенных или к сотовому маршрутизатору, который связывается со смотрящей в небо сети сотовых вышек на земле, или к спутниковому маршрутизатору, который подключается к спутнику, чтобы передать данные на спутник, а затем на наземную станцию. Система на основе сотовой связи требует наличие сети наземных сотовых приемников; следовательно, она не используется для полетов, пересекающих океан. Этот предлагаемый на борту сервис обычно предлагается за номинальную плату и доступен только, когда самолет летит на штатной высоте полета. Используется учет полосы, чтобы предотвратить ситуацию, когда один пользователь монополизирует соединение.

## Сети Правоохранительных Органов

Хотя Wi-Fi сети не могут предоставить покрытие широкого охвата [wide area coverage], необходимого для обеспечения непрерывной беспроводной связи, необходимой для сотрудников правоохранительных органов, они все же могут играть главную роль в борьбе с преступностью. Многие правоохранительные органы используют Wi-Fi как дополнение к своим беспроводным сетям общественной безопасности.

В дополнение к очевидным преимуществам мобильности при использовании Wi-Fi внутри полицейского участка, многие муниципалитеты установили Wi-Fi на парковках снаружи полицейских участков и других муниципальных зданий, как дополнение к беспроводным городским сетям. Эти наружные сети иногда рассматриваются как безопасные хотспоты. В отличие от публичных хотспотов, эти сети обеспечивают и аутентификацию, и высокие уровни шифрования. В дополнение к муниципалитетам, внедряющим беспроводную технологию в правоохранительные органы, многие добавляют автоматизацию, основанную не на Wi-Fi, к коммунальным услугам путем использования оборудования диспетчерского контроля и сбора данных [supervisory control and data acquisition (SCADA)]. Из-за этого роста в использовании беспроводных технологий, мы видим, что муниципалитеты назначают людей или департаменты для отслеживания используемых частот и технологий.

Муниципальные Wi-Fi хотспоты обычно предоставляют высокоскоростную связь между сетевым оборудованием в полицейском автомобиле и внутренней сетью управления отделения полиции или управления внутренних дел. Интересный пример хорошего использования этой сети – это выгрузка видео файлов с транспорта. Многие полицейские автомобили оснащены видео наблюдением, и это видео наблюдение часто используется в качестве доказательства или улики, важно не только передать эти видео файлы на центральный сервер для каталогизации и хранения, но также делать это с наименьшими действиями со стороны офицера полиции, чтобы сохранить цепочку событий.

Когда полицейский автомобиль прибывает к одному из этих муниципальных Wi-Fi хотспотов, компьютер в автомобиле автоматически загружает видео файлы с хранилища данных в автомобиле в центральную видео библиотеку. Автоматизация этого процесса минимизирует риск повреждения данных и освобождает офицера для выполнения других, более важных задач.

### Специальное Использование Полосы 4,9 ГГц

В некоторых странах полоса 4,9 ГГц выделена для использования организациями общественной безопасности и службами экстренного реагирования. Это полоса обычно требует лицензию на использование, но процесс лицензирования обычно больше формальность, чтобы гарантировать, что полоса используется надлежащим образом. Эта частота в основном внедряется и используется с наружным оборудованием, а поскольку у нее ограниченное использование, то деградация производительности от радиоинтерференции мало вероятна.

## Сети Служб Экстренного Реагирования

Когда медицинский персонал и пожарные прибывают на место происшествия, то для них важно иметь быстрый и простой доступ к необходимым ресурсам, чтобы справиться с возникшим происшествием. Многий транспорт экстренных служб оснащен или постоянно установленной Wi-Fi точкой доступа, или легко устанавливаемыми, автономными портативными точками доступа, которые могут быстро и легко подключить зону происшествия Wi-Fi мостом к сети передачи данных персонала экстренных служб. Во время стихийного бедствия, когда системы публичных услуг связи, таких как сети сотовой телефонии, могут не работать из-за перегрузки системы или выхода из строя, Wi-Fi сеть служб экстренного реагирования может обеспечить связь между персоналом на месте и, возможно, центральными ресурсами с общим доступом.

Во время стихийного бедствия или катастрофы, оценка ситуации и сортировка пострадавших (группирование пострадавших на основе степени тяжести их повреждений) является одной из первых задач. Исторически задача сортировки по очереди включает в себя бумажные метки, на которых указывают медицинскую информацию и состояние пострадавшего. Некоторые компании создали электронные сортировочные метки, которые могут содержать информацию пациента в электронном виде, и передавать ее по Wi-Fi связи.

## Провайдеры Управляемых Услуг

Растущая тенденция в отрасли информационных технологий (IT) – это обращение компаний к провайдерам управляемых услуг [*managed services provider (MSP)*]. Предполагается, что провайдер управляемых услуг (MSP) ответственен за предоставление определенного набора IT услуг своим бизнес заказчикам. Аутсорсинговые IT услуги на приватной основе часто могут улучшить работу и уменьшить затраты. Небольшие и средние предприятия [Small and medium-sized businesses (SMBs)] и корпоративные компании переносят управление и мониторинг сети в облако. Появление облачных технологий было движущей силой роста MSP для IT сетей. Многие MSP сейчас предлагают собственные облачные услуги или выступают как брокер для облачных сервисов провайдеров. Многие MSP предлагают устанавливаемые решения и решения на основе абонентской платы (подписки) по мониторингу и управлению для проводных и беспроводных сетей. Провайдеры MSP начали предлагать решения «беспроводная сеть-как-услуга» [*wireless-as-a-service (WAAS)*] под ключ своим заказчикам, использующим корпоративное сетевое оборудование БЛВС.

## Конвергенция Фиксированной и Мобильной Связи

Одна из горячих тем касательно Wi-Fi – это *конвергенция фиксированной и мобильной связи [fixed mobile convergence (FMC)]*. Цель систем FMC это предоставление одного устройства с одним телефонным номером, который способен переключаться между сетями и всегда использовать сеть с меньшей стоимостью. С гибкостью и мобильностью сотовой телефонии стало обычным для людей использовать ее даже в средах (дома или на работе), где они стационарны и у них есть доступ к другим телефонным системам, которые менее дорогие. Устройства FMC обычно способны связываться или через сотовую телефонную сеть или через VoWiFi сеть. Если у вас есть FMC телефон, и вы находитесь в офисе или дома, где есть Wi-Fi сеть, телефон будет использовать Wi-Fi сеть для всех входящих и исходящих телефонных звонков. Если вы находитесь за пределами этих мест, и у вас нет доступа к Wi-Fi сети, телефон будет использовать сотовую сеть для всех входящих и исходящих телефонных звонков. Устройства FMC также позволяют переключаться между сетями, так что вы можете начать телефонный звонок в офисе вашей компании с помощью Wi-Fi сети. А как вы выйдете наружу, FMC телефон переключиться с Wi-Fi сети на сотовую сеть и незаметно осуществит переход между двумя сетями. С фиксированной мобильной конвергенцией вы сможете иметь одно устройство и один телефонный номер, который будет работать, где бы вы ни были, используя наименее дорогую сеть, которая доступна в это время.

Пример FMC это *Wi-Fi Calling* [*произносится, как Вай-Фай Коллинг*], который позволяет смартфонам подключаться к сети мобильного оператора через Wi-Fi точки доступа. Wi-Fi Calling – это сервис смартфонов на Android и iOS, предоставляемый многими сотовыми операторами. В Wi-Fi Calling не требуется никакого отдельного приложения или логина.

## БЛВС и Здоровье

На протяжении многих лет существовала обеспокоенность о неблагоприятном влиянии на здоровье от облучения людей и животных радиоволнами. Всемирная Организация Здравоохранения [World Health Organization] и правительственные организации установили стандарты, которые устанавливают ограничения на излучения для радио волн, которым должны соответствовать радиочастотные продукты. Проводимые испытания на БЛВС показывают, что они работают существенно ниже требуемых безопасных ограничений, установленных этими организациями. Также, сигналы Wi-Fi, по сравнению с другими радиосигналами, намного меньше по мощности. Всемирная Организация Здравоохранения также заключила, что нет убедительных доказательств, что слабые радио-частотные сигналы, такие как при связи 802.11, вызывают неблагоприятное влияние на здоровье.

Вы можете прочитать больше о некоторых из этих изысканиях на следующих вебсайтах:

- **Федеральная Комиссия по Связи США [U.S. Federal Communications Commission]:** [www.fcc.gov/general/radio-frequency-safety-0](http://www.fcc.gov/general/radio-frequency-safety-0)
- **Всемирная Организация Здравоохранения [World Health Organization]:** [www.who.int](http://www.who.int)
- **Wi-Fi Альянс [Wi-Fi Alliance]:** [www.wi-fi.org](http://www.wi-fi.org)

## Интернет Вещей

Как упоминалось в Главе 11 “Архитектура БЛВС,” развертывание устройств Интернета Вещей [Internet of Things (IoT)] в виде датчиков, мониторов, и машин быстро растет. Сетевые радио карты 802.11 [NICs], используемые как клиентские устройства, стали появляться во многих типах машин и решений. Wi-Fi радиомодули уже присутствуют в игровых устройствах, стерео системах, и видеокамерах. Производители аппаратуры размещают Wi-Fi NICs в стиральных машинах, холодильниках, и автомобилях. Использование Wi-Fi радиомодулей в сенсорных и мониторинговых устройствах, также, как и RFID, имеет многочисленные применения в многочисленных корпоративных вертикальных рынках. Стоит отметить, что IoT устройства часто используют другие беспроводные сетевые технологии такие, как Bluetooth, Zigbee, и Z-Wave, вместо беспроводной технологии 802.11.

Промышленность использует IoT устройства для управления инвентарем и логистикой для улучшения производительности производства с помощью мониторинговых решений по предиктивному анализу. Решения IoT в здравоохранении в первую очередь используются для интеграции подключенных медицинских устройств и анализу данных с целью улучшения медицинского обслуживания. IoT сенсоры используются во многих отраслях для мониторинга температуры, вентиляции и систем кондиционирования воздуха в зданиях. IT администраторы должны управлять регистрацией, доступом и политиками безопасности IoT устройств, подключенных к корпоративной сети.

# Производители БЛВС

Существует много производителей на рынке БЛВС 802.11. Далее представлен список некоторых из основных производителей БЛВС. Пожалуйста, обратите внимание, что каждый производитель перечислен только в одной категории, даже если он предлагает продукты и услуги, которые охватывают несколько категорий. Это наиболее заметно с производителями инфраструктуры, кто предлагает дополнительные возможности, такие как безопасность и решение и устранение проблем, в качестве характеристик своих продуктов.

**Инфраструктура БЛВС** Следующие производители корпоративного оборудования 802.11 производят и продают контроллеры БЛВС и/или корпоративные точки доступа:

**ADTRAN** [www.adtran.com](http://www.adtran.com)

**Arista Networks** [www.arista.com](http://www.arista.com)

**Aruba Networks (подразделение HPE)** [www.arubanetworks.com](http://www.arubanetworks.com)

**Cisco Systems** [www.cisco.com](http://www.cisco.com)

**CommScope** [www.commscope.com](http://www.commscope.com)

**Extreme Networks** [www.extremenetworks.com](http://www.extremenetworks.com)

**Fortinet** [www.fortinet.com](http://www.fortinet.com)

**Huawei** [www.huawei.com](http://www.huawei.com)

**Mist Systems (подразделение Juniper Networks)** [www.mist.com](http://www.mist.com)

**Ubiquiti Networks** [www.ubnt.com](http://www.ubnt.com)

**Внешние Взаимосвязные [Mesh] или Транзитные [Backhaul] БЛВС** Следующие производители БЛВС специализируются на наружных взаимосвязанных [mesh] сетях 802.11 или наружных беспроводных мостах:

**Airspan** [www.airspan.com](http://www.airspan.com)

**Cambium Networks** [www.cambiumnetworks.com](http://www.cambiumnetworks.com)

**Meshdynamics** [www.meshdynamics.com](http://www.meshdynamics.com)

**Proxim Wireless** [www.proxim.com](http://www.proxim.com)

**Strix Systems** [www.strixsystems.com](http://www.strixsystems.com)

**Антennы и аксессуары БЛВС** Следующие компании делают и/или продают антенны БЛВС, корпуса и решения для монтажа, и аксессуары:

**AccelTex Solutions** [www.acceltex.com](http://www.acceltex.com)

**Oberon** [www.oberoninc.com](http://www.oberoninc.com)

**PCTEL** [www.pctel.com](http://www.pctel.com)

**Ventev** [www.ventev.com](http://www.ventev.com)

**Решения по проектированию БЛВС и решению проблем на БЛВС** Следующие компании делают и/или продают анализаторы протокола 802.11, анализаторы спектра, программное обеспечение по обследованию, решения RTLS и другие инструменты анализа и решения проблем БЛВС:

**7signal** [www.7signal.com](http://www.7signal.com)

**Berkeley Varitronics Systems** [www.bvsystems.com](http://www.bvsystems.com)

**Ekahau** [www.ekahau.com](http://www.ekahau.com) **iBwave**

[www.ibwave.com](http://www.ibwave.com)

**LiveAction** [www.liveaction.com](http://www.liveaction.com)

**MetaGeek** [www.metageek.net](http://www.metageek.net)

**NETSCOUT** [www.netscout.com](http://www.netscout.com)

**nutsaboutnets** [www.nutsaboutnets.com](http://www.nutsaboutnets.com)

**Stanley Healthcare** [www.stanleyhealthcare.com](http://www.stanleyhealthcare.com)

**TamoSoft** [www.tamos.com](http://www.tamos.com)

**Wireshark** [www.wireshark.org](http://www.wireshark.org)

**Zebra Technologies** [www.zebra.com](http://www.zebra.com)

**Решения по безопасности БЛВС и управления гостями** Следующие компании предлагают решения по управлению гостевыми БЛВС, решениями по регистрации клиентов в сети, или клиентские решения 802.1X/EAP:

**Cloud4Wi** [www.cloud4wi.com](http://www.cloud4wi.com)

**Cucumber Tony** [www.ct-networks.io](http://www.ct-networks.io)

**GoZone WiFi** [www.gozonewifi.com](http://www.gozonewifi.com)

**Kiana** [www.kiana.io](http://www.kiana.io)

**Purple** [www.purple.ai](http://www.purple.ai)

**SecureW2** [www.secureW2.com](http://www.secureW2.com)

**Решения VoWiFi** Производители телефонов 802.11 VoWiFi и VoIP шлюзов включают следующих:

**Ascom** [www.ascom.com](http://www.ascom.com)

**Mitel** [www.mitel.com](http://www.mitel.com)

**Spectralink** [www.spectralink.com](http://www.spectralink.com)

**Vocera** [www.vocera.com](http://www.vocera.com)

**Производители Систем Управления Мобильными Устройствами(MDM)** Далее перечислены некоторые из производителей, продающих решения по управлению мобильными устройствами (MDM):

**AirWatch** [www.air-watch.com](http://www.air-watch.com)

**Jamf** [www.jamf.com](http://www.jamf.com)

**MobileIron** [www.mobileiron.com](http://www.mobileiron.com)

**Производители потребительского Wi-Fi** Далее идут некоторые из многочисленных производителей БЛВС, продающих решения потребительского класса, которые могут предоставить Wi-Fi среднестатистическому домашнему пользователю:

**Asus** [www.asus.com](http://www.asus.com)

**Buffalo Technology** [www.buffalo-technology.com](http://www.buffalo-technology.com)

**D-Link** [www.dlink.com](http://www.dlink.com)

**eero (подразделение Amazon)** [www.eero.com](http://www.eero.com)

**Google** [www.google.com](http://www.google.com)

**Hawking Technology** [www.hawkingtech.com](http://www.hawkingtech.com)

**Linksys** [www.linksys.com](http://www.linksys.com)

**NETGEAR** [www.netgear.com](http://www.netgear.com)

**Plume** [www.plumewifi.com](http://www.plumewifi.com)

**TP-Link** [www.tp-link.com](http://www.tp-link.com)

**Zyxel** [www.zyxel.com](http://www.zyxel.com)

## ИТОГО

Эта глава охватывает немного из проектирования, внедрения и управления для сред, в которых используются беспроводные сети. Хотя многие из этих сред похожи, каждая имеет уникальные характеристики. Важно понимать эти сходства и различия, и как обычно разворачиваются беспроводные сети.

## Темы Экзамена

**Знать разные вертикальные рынки БЛВС.** Беспроводные сети могут использоваться во многих средах, каждый вертикальный рынок имеет отличную от других основную причину или фокус для установки беспроводной сети. Знать эти среды и их основные причины для установки беспроводной сети 802.11.

## Контрольные Вопросы

1. Какие из этих технологий могут использоваться устройствами IoT? (Выберите все, что применимо.)

  - A. Wi-Fi
  - B. Bluetooth
  - C. Zigbee
  - D. Ethernet
2. Какой тип идентификатора используется радиомодулями BLE для целей зон непосредственной близости iBeacon?

  - A. BSSID
  - B. UUID
  - C. SSID
  - D. PMKID
3. Какой тип мест часто имеет персону, ответственную за контроль использования частот внутри организации?

  - A. Производственное предприятие
  - B. Хотспот
  - C. Больница
  - D. Круизный корабль
4. На какой из этих транспортных сетях спутник является рабочим решением для предоставления канала подключения к сети Интернет?

  - A. Автобус
  - B. Автомобиль
  - C. Поезд
  - D. Круизный корабль
5. Фиксированная мобильная конвергенция предоставляет роуминг между какими из следующих беспроводных технологий? (Выберите все, что применимо.)

  - A. Bluetooth
  - B. Wi-Fi
  - C. WiMAX
  - D. Сотовая
6. Что из перечисленного далее является типовой самой важной целью проекта при проектировании БЛВС склада?

  - A. Емкость [Capacity]
  - B. Пропускная способность [Throughput]
  - C. Радиоинтерференция [RF interference]
  - D. Покрытие [Coverage]

7. Бобу была поставлена задача развернуть БЛВС в местной 12 летней школьной системе. Однако государственные представители обеспокоены тем, что радиоволновая энергия от Wi-Fi радиомодулей приведет к заболеванию детей и, возможно, к свечению в темноте. Как должен поступить Боб с обеспокоенностью чиновников?
- A. Пообещать установить уменьшающие излучение щиты на каждой точке доступа.
  - B. Предоставить отзывы здоровых школьников, которые пользовались Wi-Fi.
  - C. Рекомендовать всем школьникам уйти на карантин домой, пока не появится вакцина от Wi-Fi.
  - D. Направить обеспокоенных лиц на отчеты о медицинских исследованиях, доступные на сайтах Wi-Fi Альянса и Всемирной Организации Здравоохранения.
8. Какой тип сервис провайдеров предлагает решения беспроводная сеть-как-услуга [ wireless-as-a-service (WAAS)] «под ключ» своим заказчикам, использующим сетевое оборудование БЛВС корпоративного класса?
- A. WISP
  - B. ISP
  - C. MSP
  - D. WISPs
9. Что из следующего является главной задачей сети 802.11 SOHO?
- A. Общая сеть
  - B. Шлюз в Интернет
  - C. Домашняя сетевая безопасность
  - D. Общий доступ для печати
10. Какой тип решения VPN обычно устанавливается на удаленной ТД дома удаленного сотрудника?
- A. IPsec VPN 2ого Уровня
  - B. PPTP VPN 3его Уровня
  - C. IPsec VPN 3его Уровня
  - D. SSL VPN 7ого Уровня
11. Складские и производственные среды обычно имеют какие из перечисленных далее требований? (Выберите все, что применимо.)
- A. Мобильность
  - B. Высокоскоростной доступ
  - C. Высокая емкость
  - D. Широкое покрытие
12. Что необходимо, чтобы запустить действие на мобильном устройстве в решении зоны непосредственной близости iBeacon? (Выберите все, что применимо.)
- A. Передатчик 802.11
  - B. Приложение

- C. Передатчик BLE
  - D. Шифрование данных
13. Что из следующего является хорошим использованием для портативных сетей? (Выберите все, что применимо.)
- A. Военные маневры
  - B. Устранение последствий стихийных бедствий
  - C. Территории строительства
  - D. Производственные заводы
14. Какой из следующих терминов относится к сетевому дизайну PtMP? (Выберите все, что применимо.)
- A. PtP
  - B. Mesh [Взаимосвязанный]
  - C. Hub and spoke [Ступица и спицы]
  - D. Star [Звезда]
15. Самые ранние установки устаревших ТД 802.11 FHSS использовались в каких типах сред?
- A. Мобильные офисные сети
  - B. Образовательные среды/Классы
  - C. Промышленные среды(складские и производственные)
  - D. Здравоохранение (больницы и офисы)
16. При использовании БЛВС хотспота, что должны делать сотрудники компании из следующего, чтобы гарантировать безопасное подключение к вашей корпоративной сети?
- A. Включить WEP.
  - B. Включить 802.1X/EAP.
  - C. Использовать IPsec VPN.
  - D. Безопасность не может быть обеспечена, потому что вы не контролируете точку доступа.
17. Какие некоторые популярные приложения 802.11 используются в здравоохранении? (Выберите все, что применимо.)
- A. VoWiFi
  - B. Мост
  - C. RTLS
  - D. Мониторинг пациентов
18. Двойные мосты точка-точка между одними и теми же местами часто устанавливаются по каким из далее перечисленных причинам? (Выберите все, что применимо.)
- A. Чтобы предоставить более высокую пропускную способность
  - B. Чтобы предотвратить перекрытие каналов

- C. Чтобы устраниить единую точку отказа
  - D. Чтобы включить поддержку VLANов
19. Какие из ключевых вопросов/целей поставщиков медицинских услуг при установке беспроводной сети? (Выберите все, что применимо.)
- A. Радиоинтерференция
  - B. Быстрый доступ к данным пациента
  - C. Безопасный и надежный доступ
  - D. Мобильность
20. При предоставлении удаленного беспроводного доступа с помощью филиального маршрутизатора БЛВС и IPSec VPN Зого Уровня, откуда обычно выдаются клиентские IP адреса?
- A. DHCP сервер в корпоративной штаб квартире
  - B. Локальный DHCP сервер в офисе филиала
  - C. Внутренний DHCP сервер в филиальном БЛВС маршрутизаторе
  - D. Статические IP адреса



**Приложение**

**A**



# **Ответы на Контрольные Вопросы**

# Глава 1: Обзор Беспроводных Стандартов, Организаций и Основ

1. С. Беспроводные сети 802.11, обычно, используются для подключения клиентских станций к сети через точку доступа. Точки доступа устанавливаются на уровне доступа [access], а не на уровне ядра [core] или распределения [distribution]. Физический уровень - это уровень модели OSI, а не уровень сетевой архитектуры.
2. Е. Радиосвязь регулируется по-разному во многих регионах и странах. Политику использования спектра и правила мощности передачи определяют местные регулирующие организации отдельных стран или регионов.
3. В. Беспроводные мосты 802.11 обычно используются для осуществления работы на уровне распределения [distribution layer]. Устройства уровня ядра обычно намного быстрее, чем беспроводные устройства 802.11, но и мосты не используются для предоставления сервисов уровня доступа. Сетевой уровень - это уровень модели OSI, а не уровень сетевой архитектуры.
4. А. Институт Инженеров Электротехники и Электроники [Institute of Electrical and Electronics Engineers (IEEE)] отвечает за создание всех стандартов 802.
5. D. Wi-Fi Альянс обеспечивает сертификационные испытания, а когда продукт проходит тест, то он получает сертификат совместимость с Wi-Fi [Wi-Fi Interoperability Certificate].
6. С. Несущий сигнал - это модулированный сигнал, который используется для передачи двоичных данных.
7. В. Из-за влияния шума на амплитуду сигнала, Амплитудную Модуляцию [amplitude-shift keying (ASK)] следует использовать с осторожностью.
8. С. Стандарт IEEE 802.11-2020 определяет механизмы связи только на Физическом уровне [Physical layer] и MAC подуровне Канального уровня [Data-Link layer] модели OSI. Подуровень Контроля Логического Канала Связи [Logical Link Control (LLC)] Канального уровня [Data-Link layer] не определен для работы 802.11. PLCP и PMD являются подуровнями Физического уровня.
9. Е. IETF ответственно за создание документов RFC. IEEE отвечает за стандарты 802. Wi-Fi Альянс отвечает за сертификационные испытания (тесты). Wi-Fi Альянс изначально назывался WECA, но изменил свое имя на Wi-Fi Альянс в 2002 году. FCC отвечает за правила радиочастотного регулирования в Соединенных Штатах.
10. А, С, Е. Плоскость управления существует для мониторинга и администрирования телекоммуникационной сети. Плоскость контроля характеризуется как интеллект сети. Плоскость данных переносит сетевой пользовательский трафик.
11. А, В, С. Три метода модуляции [keying methods], которые могут использоваться для кодирования данных - это амплитудная модуляция [amplitude-shift keying (ASK)], частотная модуляция [frequency-shift keying (FSK)], и фазовая модуляция [phase-shift keying (PSK)].
12. В, Е. Стандарт IEEE 802.11-2020 определяет механизмы связи только на Физическом уровне [Physical layer] и MAC подуровне Канального [Data-Link] уровня модели OSI.

13. С. Высота [Height] и мощность [power] - это два термина, который описывают амплитуду волны. Частота - это как часто волна повторяется. Длина волны - это реальная длина волны, обычно измеряемая от пика до пика. Фаза указывает на стартовую точку волны в сравнении с другой волной.
14. В. СЕРТИФИЦИРОВАННЫЙ Wi-Fi 6 [Wi-Fi CERTIFIED 6] сертифицирует рабочие возможности для радиомодулей 802.11ax для обеих полос частот 2,4 ГГц и 5 ГГц. Wi-Fi 6E - это расширение Wi-Fi 6 для сертификации радиомодулей 802.11ax в 6 ГГц полосе частот.
15. А. IETF создает RFCs, IEEE создает стандарты 802, Wi-Fi Альянс предоставляет СЕРТИФИЦИРОВАННЫЕ Wi-Fi [Wi-Fi CERTIFIED] стандарты, а ITU-R определяет регионы радиорегулирования. Регулирующие организации управляют регуляторными правилами в своем регионе.
16. А, В, С, Д, Е. Все они обычно регулируются локальными или региональными радиочастотными регулирующими организациями.
17. В. В полудуплексной связи оба устройства способны передавать и принимать; однако, только одно устройство может передавать одновременно. Рации или приемо-передающие радиостанции являются примерами полудуплексных устройств. Вся радиосвязь по природе полудуплексная. Радиомодули БЛВС IEEE 802.11 используют полудуплексную связь.
18. Д. Волна делится на 360 градусов.
19. В, С. Основное преимущество нелицензируемой частоты в том, что разрешение на передачу на частоте бесплатно, и в том что любой может использовать нелицензируемую частоту. Хотя и нет дополнительных финансовых затрат, вы должны продолжать следовать регуляторным правилам по передаче и другим ограничениям. Тот факт, что любой может использовать полосу частот, также является недостатком из-за переполненности.
20. С. Модель OSI иногда называется как семиуровневая модель.

## Глава 2: Стандарт и Поправки IEEE 802.11

1. Е. 802.11ah определяет использование Wi-Fi на частотах ниже 1 ГГц, и является основой для сертификации Wi-Fi HaLow. Низкие частоты обеспечивают более длинные расстояния, что будет определенно полезно для датчиков, IoT устройств, и связи машина-машина (M2M).
2. В. 802.11ad поддерживает скорости передачи данных до 7 Гбит/с. Обратная сторона в том, что у 60 ГГц будет значительно меньшее фактическое расстояние работы, чем у 5 ГГц сигнала, и связь будет ограничена прямой видимостью, так как сигналам с высокой частотой сложнее проникать через стены. Ожидается, что черновая поправка 802.11ay улучшит 802.11ad, предоставляя более высокие скорости и более длинные расстояния.
3. В, D, Е. Исходный стандарт 802.11 определял три спецификации Физического уровня Устаревшие сети 802.11 могли использовать технологии: расширение спектра с перестройкой частоты [frequency-hopping spread-spectrum (FHSS)],

расширение спектра прямой последовательностью [direct-sequence spread-spectrum (DSSS)], или инфракрасную связь [IR (infrared)]. 802.11b определяла использование Высокоскоростное DSSS [High-Rate DSSS (HR-DSSS)]; 802.11a определяла использование ортогонального мультиплексирования с частотным разделением [orthogonal frequency-division multiplexing (OFDM)]; 802.11g определяла Физическое Расширение Скорости [Extended Rate Physical (ERP)]; 802.11n определяла Высокую Пропускную Способность [High Throughput (HT)]; 802.11ac определяла Очень Высокую Пропускную Способность [Very High Throughput (VHT)]; а 802.11ax определяет Высокую Эффективность [High Efficiency (HE)].

4. С. Рабочая Группа 802.11 по задаче s [802.11 Task Group s (TGs)] отправилась в путь по стандартизации взаимосвязанных [mesh] сетей с помощью уровней MAC/PHY IEEE 802.11. Поправка 802.11s определяет использование взаимосвязываемых точек [mesh points (MPs)], которые являются станциями 802.11 с поддержкой QoS, которые поддерживают сервисы взаимосвязанности [mesh]. MP [взаимосвязываемые точки] способны использовать обязательный протокол взаимосвязываемой маршрутизации [mesh routing protocol], который называется, как Гибридный Беспроводной Взаимосвязываемый Протокол [Hybrid Wireless Mesh Protocol (HWMP)], который использует метрики выбора пути по умолчанию [default path selection metric]. Производители могут также использовать проприетарные протоколы и метрики взаимосвязанной [mesh] маршрутизации.
5. D, F. Требуемый метод шифрования, определенный беспроводной сетью RSN (802.11i) - это Протокол Режима Счетчика с Кодом Аутентификации из Шифрованных Блоков Цепочки Сообщений [Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)], который использует алгоритмы Стандарта Улучшенного Шифрования [Advanced Encryption Standard (AES)]. Поправка 802.11i также требует использование решения по аутентификации 802.1X/EAP или использовать заранее известные ключи [preshared keys].
6. D. Радиокарты 802.11ac работают в 5 ГГц полосах частот, используя очень высокую пропускную способность [very high throughput (VHT)].
7. D. Стандарт IEEE 802.11-2020 требует скорости передачи данных в 6, 12, и 24 Мбит/с и для радиомодулей 802.11a ортогонального мультиплексирования с разделением частоты [orthogonal frequency-division multiplexing (OFDM)], и для радиомодулей 802.11g Физически Расширенной Скорости – OFDM [Extended Rate Physical OFDM (ERP-OFDM)]. Обычно поддерживаются скорости передачи данных 6, 9, 12, 18, 24, 36, 48, и 54 Мбит/с. 54 Мбит/с – это максимальная определенная скорость для этих двух технологий 802.11 (802.11a и 802.11g).
8. В. Быстрая смена базового состава сервиса (FT), также называемая, как быстрый безопасный роуминг [fast-secure roaming], определяет быструю смену обслуживающей точки [handoff], когда происходит роуминг между сотами в БЛВС с использованием сильной безопасности, определенной в надежной безопасной сети [robust security network (RSN)]. Такие приложения, как VoIP, которым необходима своевременная доставка пакетов, требуют, чтобы роуминговая смена обслуживающей точки [handoff] происходила за 150 мс или меньше.
9. В, С, Е. Вышла поправка 802.11ac и определила модуляцию 256-QAM, восемь пространственных потоков, многопользовательское MIMO (MU-MIMO), 80 МГц каналы, и 160 МГц каналы. Технология MIMO 802.11 и 40 МГц каналы появились с принятием поправки 802.11n.
10. А. Поправка 802.11af позволяет использовать частоты белого ТВ пространства [TV white space (TVWS)] между 54МГц и 790МГц. Физический уровень основан на технологии OFDM, используемой в 802.11ac, но с использованием каналов с меньшей шириной, по сравнению с 802.11ac, вместе с максимум четырьмя пространственными

потоками. Этот новый физический уровень [PHY] называется, как телевизионная очень высокая пропускная способность [television very high throughput (TVHT)], и спроектирован для поддержки узких ТВ каналов, которые доступны в TVWS.

11. А, Е. Стандарт 802.11-2020 определяет механизмы для динамического выбора частоты [dynamic frequency selection (DFS)] и контроля мощности передачи [transmit power control (TPC)], которые могут быть использованы для удовлетворения регуляторных требований для работы в 5 ГГц полосе. Технологии DFS и TPC изначально были определены в поправке 802.11h, которая теперь является частью стандарта 802.11-2020.
12. С, D. Поправки 802.11ac и 802.11ad часто называются как поправки "гигабитного Wi-Fi" ["gigabit Wi-Fi"], потому что они определяют скорости передачи данных более 1 Гбит/с. Рабочие группы по задачам 802.11ac и 802.11ad очень высокой пропускной способности [very high throughput (VHT)] определяют скорости передачи до 7 Гбит/с в среде 802.11.
13. А, С, D, Е. ERP (802.11g) требует использование Физически Расширенной Скорости в OFDM [Extended Rate Physical OFDM (ERP-OFDM)] и Физически Расширенную Скорость в DSSS [Extended Rate Physical DSSS (ERP-DSSS/CCK)] в промышленной, научной, и медицинской (ISM) полосе в 2,4 ГГц, и является обратно совместимым с оборудованием 802.11b Высоко-Скоростным DSSS [High-Rate DSSS (HR- DSSS)] и оборудованием с расширением спектра прямой последовательности [direct-sequence spread-spectrum (DSSS)]. 802.11b использует HR-DSSS в 2.4 ГГц ISM полосе и является обратно совместимым только с устаревшим DSSS оборудованием, а не устаревшим оборудованием с расширением спектра с перестройкой частоты [frequency-hopping spread-spectrum (FHSS)]. 802.11ac использует очень высокую пропускную способность [very high throughput (VHT)] и является обратно совместимым с ортогональным мультиплексированием с частотным разделением [orthogonal frequency-division multiplexing (OFDM)] 802.11a. Поправка 802.11h определяет использование контроля передачи мощности [transmit power control (TPC)] и динамический выбор частоты [dynamic frequency selection (DFS)] в 5 ГГц полосах Нелицензируемой Национальной Инфраструктуры [Unlicensed National Information Infrastructure (U-NII)] и является расширением поправки 802.11a. Технология OFDM используется со всеми 802.11a- и 802.11h-совместимыми радиомодулями.
14. Д. Поправка 802.11ac определяет максимальную скорость передачи данных в 6933.3 Мбит/с. Однако, чипсеты 802.11ac прошли через множество поколений с разными способностями. Максимальная скорость передачи данных для большинства устройств 802.11ac первого поколения составляет 1300Мбит/с, а максимальная скорость передачи данных для устройств второго поколения 802.11ac составляет 3466.7 Мбит/с. Вспомните, что скорости передачи данных не равны пропускной действительной пропускной способности.
15. В, D, Е. Исходный стандарт 802.11 определял использование Проводного Эквивалента Конфиденциальности [Wired Equivalent Privacy (WEP)] для шифрования. Исходный стандарт также определяет два способа аутентификации: аутентификация Открытой Системы [Open System authentication] и аутентификация с Общим Ключом [Shared Key authentication]. TKIP был представлен в 2002 году, чтобы решить проблемы в безопасности, обнаруженные в WEP. В 2012 году и WEP, и TKIP были убраны из стандарта.
16. А. Черновая поправка 802.11u определяет интеграцию сетей доступа IEEE 802.11 с внешними сетями в универсальной и стандартизированной манере. 802.11u часто называют, как Работа Беспроводной Сети с Внешними Сетями [Wireless Interworking with External Networks (WIEN)].
17. А, С. Поправка 802.11e (теперь часть стандарта 802.11-2020) определяла два улучшенных способа доступа к среде для поддержки требований к качеству обслуживания [quality of service (QoS)]. Расширенный Распределенный Доступ к Каналу [Enhanced Distributed Channel Access (EDCA)] является расширением к Функции

Распределенной Координации [Distributed Coordination Function (DCF)]. Доступ к Каналам, Контролируемый Функцией Гибридной Координации [Hybrid Coordination Function Controlled Channel Access (HCCA)] является расширением к PCF. В реальном мире внедрена только EDCA.

18. А, С. Поправка 802.11h представила два основных улучшения: контроль мощности передачи [transmit power control (TPC)] и динамический выбор частоты [dynamic frequency selection (DFS)] для обнаружения и избегания радара. Все аспекты принятой поправки 802.11h теперь можно найти в стандарте 802.11-2020.
19. Е. Поправка 802.11n высокая пропускная способность [high throughput (HT)] определяла улучшения для MAC(контроля доступа к среде) и PHY(физического уровня), в то время как радиомодули могут передавать на скоростях передачи данных до 600 Мбит/с.
20. В, Д. IEEE специально определяет технологии 802.11 на Физическом уровне и MAC подуровне Канального [Data-Link] уровня. По идее, все что происходит на более высоких уровнях модели OSI несущественно для связи 802.11.

## Глава 3: Основы Радиотехники

1. В, С. Многолучевое распространение может привести к затуханию, усилению, потере сигнала, или повреждению данных. Если два сигнала прибывают вместе в фазе, то результат - увеличение силы сигнала, которое называется усиливающее замирание [upfade]. Разброс задержки [delay spread] также может быть значительным и быть причиной повреждений битов данных, приводя к чрезмерным повторным передачам на 2ом уровне.
2. Д. Длина волны [wavelength] - это линейное расстояние между повторяющимися гребнями (пиками) [crests (peaks)] или повторяющимися впадинами (долинами) [troughs (valleys)] одного цикла полной волны [wave pattern].
3. В, С. Радиочастотные усилители добавляют активное усиление [active gain] с помощью внешнего источника питания. Пассивное усиление обычно создается антennами, которые фокусируют энергию сигнала без использования внешних источников питания.
4. А. Стандартная мера количества раз (циклов), которое сигнал повторится в секунду - это герц (Гц) [hertz (Hz)]. Один Гц равен одному циклу в 1 секунду.
5. Д. Часто путается с рефракцией [refraction] (преломлением) , дифракция [diffraction] (преломление) - это изгибание фронта волны вокруг препятствия. Дифракция вызывается некоторым типом блокирования радиосигнала, например, небольшим холмом или зданием, которые располагаются между передающим радиомодулем и приемником.
6. С. Если несколько копий радиосигнала от передатчика прибывает на приемник в одно и то же время, но не будет разницы по фазе. Сигналы, у которых разница по фазе равна 0 (ноль) градусов, в действительности, суммируют свои амплитуды, что приводит к тому, что у приемного сигнала намного большая сила сигнала, потенциально почти в два раза больше.
7. В, С. Когда несколько радиосигналов прибывает на приемник в одно и то же время, и они находятся в фазе или частично не в фазе с основной волной [primary wave], то результатом является увеличение силы (амплитуды) сигнала. Однако, финальный принятый сигнал, находящийся ли под действием усиливающего замирания [upfade] или уменьшающего замирания [downfade], никогда не будет сильнее, чем исходный переданный сигнал из-за затухания на пути в свободном пространстве.

8. В. Беспроводные ЛВС 802.11 работают в 60 ГГц, 6ГГц, 5ГГц, и 2.4 ГГц диапазонах частот. Однако, 2.4ГГц равно 2.4 миллиарду циклов в секунду. Частота в 2.4 миллиона циклов в секунду - это 2.4 МГц. Вопрос с подвохом!
9. А. Осциллограф - это инструмент из временной области, который может быть использован для измерения того как часто изменяется амплитуда сигнала во времени. Инструмент частотной области, называемый анализатором спектра, является обычным инструментом наиболее часто используемым в радиообследовании [site surveys].
10. А, С, D. Это сложный вопрос для ответа, потому что много одних и тех же сред могут вызывать различные виды распространения. Металл всегда относится к отражению. Вода является главным источником поглощения; однако, огромные пространства воды также могут вызывать отражение. Плоские поверхности такие, как асфальтные дороги, потолки, и стены всегда будут приводить к отражению.
11. А, В, D, F. Многолучевое распространение [Multipath]- это явление распространения, которое получается в результате двух или более путей сигнала, прибывающего на приемную антенну в одно и тоже время или в пределах нескольких наносекунд друг от друга. Из-за естественного расширения волн распространение при отражении [reflection], рассеяния [scattering], дифракции [diffraction], и преломления [refraction], все могут привести к нескольким путям [multiple paths] одного и того же сигнала. Отражение обычно считается основной причиной сред с высоким многолучевым распространением [multipath].
12. В. Рассеяние [scattering или scatter] определяется как радиосигнал отражающийся во множество направлений, при столкновении с неровной, шероховатой поверхностью.
13. А, В, С. Среды с высоким многолучевым распространением [High-multipath environments] могут иметь деструктивное влияние на передачи устаревших радиомодулей 802.11 a/b/g. Многолучевое распространение имеет конструктивное влияние на передачи в 802.11n/ac/ax, которые используют разнесение антенн MIMO и технику обработки сигналов Комбинацию Максимальных Отношений [maximum ratio combining (MRC)].
14. А, В, С, F. Расслоение воздуха [air stratification] является ведущей причиной преломления [refraction] радиосигнала. Изменения в температуре воздуха, изменения в давлении воздуха, и водяные пары вызывают преломление [refraction]. Смог может вызывать изменения плотности в давлении воздуха, а также повышение влажности.
15. А, D. Из-за естественного расширения волнового фронта, электромагнитные сигналы теряют амплитуду по мере удаления от передатчика. Скорость затухания на пути в свободном пространстве [free space path loss] является логарифмической, а не линейной. Затухание радиосигнала при прохождении через разные среды происходит, но не как функция затухания в свободном пространстве [FSPL].
16. D. Разница во времени из-за того, что отраженный сигнал проходит более длинный путь, называется как разброс задержки [delay spread]. Разброс задержки может вызвать межсимвольную интерференцию, которая приведет к повреждению данных и повторным передачам на 2ом уровне.
17. С. Анализатор спектра - это инструмент из области частот, который может быть использован для измерения амплитуды на конечном спектре частот. Осциллограф - это инструмент временной области.
18. А, С. Бетонные стены очень плотные и значительно уменьшают сигнал 2.4ГГц и 5 ГГц. Более старые строения, которые построены из стен из деревянной обрешетки и гипса, часто содержат в стенах проволочную сетку, которая используется, чтобы помочь удерживать гипс на

стенах. Проволочная сетка - хорошо известна прерыванием радиосигнала и препятствованием прохождению радиосигнала через стены. Проволочная сетка также используется в наружной лепнине. Гипсокартон уменьшает сигнал, но не в такой мере как вода, шлакоблоки или другие плотные материалы. Температура воздуха не имеет значения при обследовании места внутри помещений.

19. А. Существует обратное отношение между частотой и длиной волны. Упрощенное объяснение в том, что чем выше частота радиосигнала, тем короче будет длина волны этого сигнала. Чем длиннее длина волны радиосигнала, тем меньшая частота этого сигнала. Обе формулы содержат значение скорости света.
20. А. Преломление [Refraction] - это изгибание радиосигнала, когда он сталкивается со средой.

## Глава 4: Компоненты, Параметры, и Математика Радиосвязи

1. D. Отношение сигнал к интерференции плюс шум [signal-to-interference-plus-noise ratio (SINR)] сравнивает основной сигнал с интерференцией и шумом. Так как интерференция флукутирует и может быстро изменяться, это лучший индикатор того, что происходит с сигналов в определенном времени. Отношение сигнал-шум [signal-to-noise (SNR)] сравнивает сигнал с шумом; однако шум менее вероятно будет сильно флукутировать. Индикатор силы принятого сигнала [received signal strength indicator (RSSI)] и эквивалентная изотропно излучаемая мощность [equivalent isotropically radiated power (EIRP)] являются параметрами сигнала, но не соотносят сигнал с другими внешними влияниями.
2. Е. Изотропный излучатель также называют как точечный источник.
3. А, В, С, Е, F. При разворачивании радиосвязи, бюджет линии связи - это сумма всех усилений и затуханий (потерь) от передающего радиомодуля, через радиосреду, к приемному радиомодулю. Вычисления бюджета линии связи включают исходное усиление передачи и пассивное усиление антенны. Все потери должны быть учтены, включая затухание на пути в свободном пространстве [free space path loss]. Для вычисления затухания на пути в свободном пространстве нужны частота и расстояние. Высота антенны не имеет значения при вычислении бюджета линии связи; однако, высота может повлиять на требуемую радиоволновую линию прямой видимости, которая должна быть без препятствий для Зоны Френеля.
4. А, D. IR - это аббревиатура для расчетного излучателя [intentional radiator]. Компоненты, составляющие расчетный излучатель [IR] включают: передатчик, все кабели и разъемы, и любое другое оборудование (заземление, грозозащитники, усилители, аттенюаторы, и т.д.) между передатчиком и антенной. Мощность IR измеряется на разъеме для подключения антенны.
5. А. Эквивалентная изотропно излучаемая мощность [Equivalent isotropically radiated power], также называемая ЭИИМ [EIRP], это мера самого сильного сигнала, который излучается от антенны.
6. А, В, D. Ватты, милливатты, и дБм являются абсолютными значениями мощности. Один ватт равен одному амперу (1A) тока, текущего при 1 вольте. Милливатт - это 1/1000 от 1 ватта. дБм - это децибелы относительно 1 милливатта.
7. В, С, D, Е. Единица измерения, которая называется бел - это относительное выражение и мера изменения мощности. Децибел (dB) равен одной десятой бела. Параметры усиления антенны

дБи и дБд являются относительными мерами. дБи определяется как децибелы относительно изотропного излучателя. дБд определяется как децибелы относительно дипольной антенны.

8. С. Чтобы преобразовать любое значение дБд в дБи, просто добавьте 2.14 к значению дБд.
9. А. Чтобы преобразовать дБм[dBm] в мВт[mW], сначала вычисляем сколько 10ок и 3оэ нужно сложить, чтобы получить 23, начиная с 0 дБм это  $0 + 10 + 10 + 3$ . Чтобы вычислить мВт, начиная с 1 мВт, вы должны умножить  $1 \times 10 \times 10 \times 2$ , что дает 200 мВт. Файл ReviewQuestion9.ppt доступный для загрузки с [www.wiley.com/go/cwnasg6e](http://www.wiley.com/go/cwnasg6e), показывает процесс детально.
10. С. Чтобы достичь 100мВт, вы можете использовать 10ки и 2шки вместе с умножением и делением. Умножая начальное значение 1 мВт на две 10ки выполнит это. Это означает, что со стороны дБм вы должны добавить две 10ки к начальному значению 0 дБм, что будет равняться 20дБм. Затем вычесть 3дБ потерь на кабеле, что даст 17 дБм. Так как вы вычли 3 со стороны дБм, вы должны поделить 100 мВт на 2, получая значение в 50 мВт. Теперь добавьте 16дБи путем добавления 10ки и двух 3оек в колонке дБм, получая таким образом 33 дБм. Так как вы добавили 10 и два раза по 3, вы должны умножить 50 мВт на 10 и два раза на 2, получая в итоге 2000мВт или 2Вт. Поскольку кабель и разъемы теряют 3дБ, а антенна добавляет 16 дБи, вы можете сложить их вместе, чтобы получить общее усиление в 13 дБ; затем применить это усиление к 100 мВт передаче сигнала (умножая на 10 и затем на 2), чтобы вычислить ЭИИМ, который получится 2000мВт или 2 Вт. Файл ReviewQuestion10.ppt, доступный для загрузки с [www.wiley.com/go/cwnasg6e](http://www.wiley.com/go/cwnasg6e), показывает процесс детально.
11. А. Если исходная мощность передачи 400 мВт, а кабель вносит 9дБ потерь, то мощность с другого конца кабеля будет 50 мВт. Первые 3 дБ потерь в кабеле уполовинят абсолютное значение мощности до 200 мВт. Вторые 3 дБ потерь в кабеле уполовинят абсолютное значение мощности до 100 мВт. Финальные 3 дБ потерь в кабеле уполовинят мощность до 50 мВт. Антенна 19 дБи пассивно усилит 50 мВт сигнал до 4000 мВт. Первые 10 дБи усиления антенны поднимут сигнал до 500 мВт. Следующие 9 дБи усиления антенны удвоят сигнал трижды до итогового значения в 4 Вт. Посколько потери в кабеле 9дБ, а усиление антенны 19 дБи, вы могли бы сложить их вместе для получения общего усиления в 10 дБ, а затем применить это усиление к 400 мВт передаче сигнала (умножая на 10), чтобы вычислить, что ЭИИМ равен 4000 мВт или 4 Вт.
12. В, D. Пороги индикатора силы принятого сигнала [Received signal strength indicator (RSSI)] является ключевым фактором для клиентов, когда они инициируют роуминговое переключение [roaming handoff]. Пороги RSSI также используются производителями для реализации динамического переключения скорости, которое является процессом, используемым радиомодулями 802.11 для переключения между скоростями передачи данных.
13. А. Индикатор силы принятого сигнала [received signal strength indicator (RSSI)] является метрикой, используемой радиокартами 802.11, чтобы измерить силу (амплитуда) сигнала. Некоторые производители используют проприетарную шкалу, чтобы также соотносить с качеством сигнала. Большинство производителей ошибочно определяют качество сигнала как отношение сигнал-шум [signal-to-noise ratio (SNR)]. Отношение сигнал-шум – это разница в децибелах между принятым сигналом и фоновым шумом (уровнем шума).
14. В. дБи определяется как “усиление в децибелах относительно изотропного излучателя” или “изменение в мощности относительно антенны.” дБи является наиболее типовым параметром усиления антенны.
15. А, F. Четыре правила 10и и 3х: На каждые 3 дБ усиления (относительного), удваивается абсолютное значение мощности (мВт). На каждые 3 дБ уменьшения (относительного), уполовинивание абсолютной мощности (мВт). На каждые 10 дБ усиления (относительного),

**992      Приложение А • Ответы на Контрольные Вопросы**

умножение абсолютной величины мощности (мВт) на множитель 10. На каждые 10 дБ уменьшения (относительного), делить абсолютную мощность (мВт) на 10.

- 16.** В. Если исходная мощность передачи была 100 мВт, а кабель вносил 3 дБ потерь, мощность на другом конце кабеля будет 50 мВт. 3 дБ потерь в кабеле уполовинивает абсолютную мощность до 50 мВт. Антенна с усилением в 10 дБи поднимет сигнал до 500 мВт. Мы также знаем, что 3 дБ потерь уполовинивает абсолютную мощность. Следовательно, антенна с усилением 7 дБи усиливает сигнал в половину, того как усиливает антенна с 10 дБи. Антенна с усилением 7 дБи пассивно усиливает 50 мВт сигнал до 250 мВт.
- 17.** D. Расстояние в 100 метров вызовет затухание на пути в свободном пространстве [free space path loss (FSPL)] в 80 дБ, намного большее, чем любая другая компонента. Радиокомпоненты такие, как разъемы, грозоразрядники, и кабель вносят потери. Однако, FSPL всегда будет причиной самых больших потерь (самого большого затухания).
- 18.** В. Правило 6 дБ гласит, что увеличение усиления на 6 децибел удваивает рабочее расстояние радиосигнала. Правило 6 дБ очень полезно для понимания усиления антенны, потому что каждые 6 дБи дополнительного усиления антенны удваивают расстояние приемлемой работы радиосигнала.
- 19.** D. В шумной среде с высоким многолучевым распространением типовой передовой опыт – то добавит 5-10 дБ запас на замирание при проектировании БЛВС мостов на основе рекомендованной производителем силы сигнала или уровня шума, смотря что сильнее.
- 20.** D. Производители БЛВС используют метрики индикатора силы принятого сигнала [received signal strength indicator (RSSI)] собственным (проприетарным) способом. Действительный диапазон значения RSSI от 0 до максимального значения (меньшего или равного 255), которое каждый производитель выбирает по своему усмотрению (оно называется RSSI\_Max). Следовательно, метрики RSSI не следует использовать при сравнении радиомодулей разных производителей БЛВС, потому что не существует стандартного диапазона значений или полноценной шкалы.

## Глава 5: Радиосигнал и Основы Теории Антенн

1. A, C, F. Азимутальная диаграмма - это вид сверху вниз на диаграмму направленности антенны, которую также называют как H-плоскость [H-plane] или горизонтальным видом. Вид сбоку называется как диаграмма по углу места [elevation chart], вертикальный вид или E-плоскость [E-plane].
2. A. Азимут - это вид сверху вниз на диаграмму направленности антенны, который также называется как H-плоскость [H-plane].
3. C. Ширина луча - это расстояние в градусах между точкой -3 дБ (половинной мощности) с одной стороны основного сигнала и точкой -3 дБ с другой стороны основного сигнала, измеряемое вдоль горизонтальной оси. Эти точки также называются как точки половинной мощности.
4. C, D. Параболическая тарелка и сетчатая антенна являются узконаправленными. Оставшиеся антенны являются полунаправленными, а секторная антенна - это особый вид полунаправленной антенны.
5. A, C, D. Полунаправленные антенны предоставляют очень широкую ширину луча [beamwidth] для поддержки связи на длинные расстояния, но будут работать и на

короткие расстояния. Они также полезны для предоставления одностороннего покрытия от точки доступа в сторону клиентов внутри помещений. Они также используются для предоставления целевого покрытия в средах с высокой плотностью.

6. В. Все что вторгается более чем на 40 процентов в зону Френеля, вероятнее всего сделает канал не надежным. Чем чище зона Френеля, тем лучше. В идеале зона Френеля вообще не должна быть заграждена.
7. С, D. Расстояние и частота определяют размер зоны Френеля; это единственное параметры в формуле зоны Френеля.
8. В. Расстояние при котором должна учитываться кривизна земли при установке канала связи точка-точка - 7 миль (11,27 км).
9. А, С. Установка более короткого кабеля определенного класса приведет к уменьшению потерь, и таким образом, большая амплитуда будет передаваться через антенну. Кабель более высокой категории, предназначенный для меньших потерь дБ, даст тот же результат.
10. В. Передатчик МIMO может передавать с нескольких антенн в то же самое время, если он работает с использованием нескольких радиоцепей.
11. А, С, D. Канал связи мост точка-точка требует минимальную чистоту зоны Френеля в 60 процентов, хотя идеально 100 процентная чистота. Полунаправленные антенны используются для каналов связи - мостов на короткие расстояния. Узконаправленные антенны используются для каналов мостов на длинные расстояния. Компенсация изгиба земли обычно не учитывается на расстояния до 7 миль (11,27 км). В каждой стране есть специфичные правила регулирования вне помещений, которые требуется соблюдать.
12. С. Коэффициент стоячей волны по напряжению (KCBH) [Voltage standing wave ratio (VSWR)] это разница между этими напряжениями и представлено в виде отношения, как 1.5:1.
13. А, С, D, E. The Отраженное напряжение, вызванное несовпадением волнового сопротивления [impedance], может привести к уменьшению мощности или амплитуды (затухание) сигнала, которые предполагается к передаче. Если передатчик не защищен от чрезмерной отраженной мощности или больших пиков мощности, он может перегреться и сломаться. Поймите, что KCBH [VSWR] может вызвать уменьшенную силу сигнала, непредсказуемую силу сигнала, или даже повреждение передатчика.
14. А, В, D, F. Частота и расстояние нужны для определения зоны Френеля. Визуальная линия прямой видимости не нужна до тех пор, пока у вас есть радиочастотная линия прямой видимости [RF line of sight]. Вы можете не видеть антennы изза тумана, но туман не препятствует радиоволновой линии прямой видимости. Земной изгиб нужно учитывать. Ширина луча не нужна для определения высоты, хотя она полезна при наведении антennы.
15. А, D. Кабели должны быть выбраны так, чтобы поддерживать используемую вами частоту.
16. А, В, С, D. Все являются возможными характеристиками радиочастотных усилителей.
17. А, В, D. Добавление аттенюатора является преднамеренным действием, чтобы добавить потери в сигнал. Поскольку кабель добавляет потери, то увеличение длины, добавит больше потерь, в то время как уменьшение длины уменьшит потери. Кабели лучшего качества дают меньшее затухание сигнала.
18. С. Грозоразрядники [Lightning arrestors] не останавливают прямой удар молнии, а только кратковременных токов [transient currents] вызванных близким ударом

19. В, Д. Область внутри радиуса первой зоны Френеля находится в фазе с точечным источником. TheRadius первой зоны Френеля - это точка, где начинается вторая зона Френеля, и где сигнал переходит из состояния в фазе с точечным источником в состояние не в фазе с точечным источником. Так как вторая зона Френеля начинается, где заканчивается вторая зона Френеля, то радиус второй зоны Френеля больше чем радиус первой зоны Френеля. Размер зоны Френеля зависит от частоты и расстояния канала связи. Усиление антенны не имеет отношения к размеру зоны Френеля.
20. Д. Боковые лепестки [Side lobes] это области покрытия антенны (отличные от покрытия, предоставляемого основным сигналом), которые имеют более сильный сигнал, чем это ожидалось при сравнении с областями вокруг них. Боковые лепестки лучше всего видны на азимутальной диаграмме. Боковые полосы и частотные гармоники не имеют ничего общего с покрытием антенны.

## Глава 6: Беспроводные Сети и Технологии Расширения Спектра

1. С. OFDM имеет большую терпимость к разбросу задержки [delay spread] по сравнению с предыдущими методами такими, как FHSS, DSSS, и HR-DSSS.
2. В, Д. Спектральная маска передачи, также называется, как спектральная маска, используется для определения ограничений спектральной плотности передач БЛВС 802.11. Иногда на спектральную маску ссылаются как на форму канала.

Наоборот, постарайтесь думать о спектральной маске, как о ширине частот, при которой мощность сигнала должна уменьшиться на определенное значение.

3. А. Модуль вектора ошибок [Error vector magnitude (EVM)] – это мера, используемая для количественной оценки производительности радиоприемника или передатчика в отношении точности модуляции. В модуляции QAM, EVM – это мера того, насколько далеко принятый сигнал от идеальной точки местоположения в созвездии. Еще один способ описать EVM – это на сколько точки созвездия сигнала отклоняются от идеального местоположения.
4. А, В, Д. Стандарт IEEE 802.11-2020 определяет, что радиомодули 802.11n HT могут передавать в полосе ISM 2.4ГГц и во всех четырех на текущий момент 5 ГГц U-NII полосах.
5. С. 20МГц OFDM каналы содержат 64 поднесущие (64 тона), но только 48 из них используются для передачи модулированных данных между радиомодулями 802.11a/g. Двенадцать из 64 поднесущих в 20 МГц канале не используются и служат защитной полосой, а четыре поднесущие работают в качестве контрольных [pilot] несущих. Радиомодули 802.11n/ac также передают в 20 МГц канале, который состоит из 64 поднесущих; однако, только 8 поднесущих являются защитными полосами. Пятьдесят две поднесущие используются для передачи модулированных данных, а четыре поднесущие выступают в качестве контрольных [pilot] несущих.
6. Д. В начале 2020 года FCC неанонимно проголосовала за то, чтобы сделать 1200 мегагерц спектра в полосе 6 ГГц доступной для безлицензионного использования в Соединенных Штатах. Это будет 59 новых 20 МГц каналов, доступных в 4x U-NII полосах (включая U-NII-5). Производители БЛВС будут строить точки доступа Wi-Fi 6E во множестве разных форм факторах, но в большинстве случаев у них будут радиомодули всех трех полос (2.4, 5 и 6 ГГц). Однако, только новые клиентские устройства Wi-Fi 6E с радиомодулями 6 ГГц будут

способны взаимодействовать с 6 ГГц радиомодулями в точке доступа Wi-Fi 6E. Старые двухчастотные (2.4 и 5 ГГц) смартфоны будут способны взаимодействовать только с 2.4 или 5 ГГц радиомодулями в трех полосной ТД Wi-Fi 6E.

7. А. Ширина полосы частот, используемая стандартным OFDM каналом примерно 20 МГц (в соответствии со спектральной маской). Однако, радиомодули 802.11n/ac/ax имеют возможность объединять 20 МГц каналы вместе. 40 МГц каналы – это фактически два 20 МГц OFDM канала, которые объединены вместе. 40 МГц спектральная маска выглядит идентично 20 МГц спектральной маске, кроме того, что она в два раза шире. Спектральная маска 80 МГц канал выглядит аналогично 20 МГц спектральной маске, кроме того, что она в четыре раза шире.
8. С. Время, которое передатчик ждет перед перестроением на следующую частоту, называется время жизни или время передачи [dwell time]. Время перестроения [hop time] – это не требуемое время, а скорее мера того, как долго происходит перестройка (скакок) [hop].
9. В. Поправка 802.11a, которая изначально определяла использование OFDM, требовала только 20 МГц расстояния между центральными частотами каналов, чтобы считаться неперекрывающимися. Все 25 каналов в 5 ГГц U-NII полосах используют OFDM и имеют расстояние в 20 МГц. Следовательно, все 5 ГГц OFDM каналы считаются непересекающимися согласно IEEE. Однако, следует отметить, что смежные 5 ГГц каналы в действительности имеют некоторое перекрытие боковых несущих частот.
10. А, D, E, F. Wi-Fi радиомодули, которые на текущий момент передают в 5 ГГц U-NII полосах, включают радиомодули, которые используют следующие технологии: 802.11a, 802.11n, 802.11ac, и 802.11ax.
11. F. Хотя FCC отклоняет расширение Wi-Fi в полосу U-NII-2B, все еще остается возможность для дополнительного расширения частоты в верхнюю часть 5 ГГц полосы. Полоса частот U-NII-4, 5.85 ГГц–5.925 ГГц, все еще рассматривается для возможного использования для Wi-Fi связи. FCC рассматривает изменение целевого использования нижних 45 МГц полосы U-NII-4 для использования для Wi-Fi и нелицензируемого использования. Верхние 40 МГц полосы U-NII-4 заново утверждены для автомобильной ITS с использованием сотовой LTE технологии, которая называется C-V2x. *Сотовая связь транспортное средство-со-всем [ Cellular vehicle-to-everything (C-V2X)]* – это технология ITS (интеллектуальной транспортной системы), предназначенная позволить транспортным средствам взаимодействовать друг с другом и всем, что вокруг (например: светофор). FCC также пересматривает должна ли старая технология автомобильной ITS, которая называется Выделенная Связь на Короткие Расстояния [Dedicated Short Range Communication (DSRC)], быть еще разрешена в полосе U-NII-4.
12. В. Если разброс задержки [delay spread] слишком велик, то данные из отраженного сигнала могут помешать тому же самому потоку данных основного сигнала; то называется межсимвольной интерференцией [intersymbol interference (ISI)]. Причина проблемы в том, что разброс задержки вызывает межсимвольную Интерференцию, которая вызывает повреждение данных.
13. Д. Стандарт 802.11-2020 гласит, что “физический уровень [PHY] OFDM должен работать в полосе 5 ГГц, в соответствии выделенными частотами регулирующей организацией в своем регионе работы.” Всего двадцать пять 20 МГц каналов доступны в 5 ГГц U-NII полосах.
14. Д. Из-за более низких скоростей передачи данных поднесущих, разброс задержки занимает меньший процент символьного периода, что означает, что менее вероятно, что произойдет ISI (межсимвольная интерференция). Другими словами, технология OFDM более устойчива к негативным ффектам

15. С. Способ доступа к среде, который называется Множественный Доступ с Контролем Несущей и Предотвращением Конфликтов [Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)] помогает гарантировать, что только один радиомодуль может передавать в любое определенное время. В зависимости от условий сети БЛВС, агрегированная пропускная способность БЛВС обычно составляет 50 процентов от рекламируемой скорости передачи данных 802.11, из-за служебной информации [overhead] при борьбе за среду. Скорости передачи данных 802.11 не являются пропускной способностью TCP. Протокол борьбы за среду CSMA/CA потребляет много из доступной полосы пропускания. В лабораторных условиях, пропускная способность TCP в среде 802.11 n/ac составляет 60-70 процентов от скорости передачи данных между ТД и одним клиентом. Значения агрегированной пропускной способности значительно ниже в средах из реальной жизни с активным участием нескольких Wi-Fi клиентов, работающих через ТД.
16. В, С, D, F. Радиомодули Wi-Fi, которые на текущий момент передают в 2.4 ГГц полосе ISM, включают радиомодули, которые используют следующие технологии: 802.11b, 802.11g, 802.11n, и 802.11ax.
17. С. В 2009 году Федеральное Управление Гражданской Авиации США [Federal Aviation Authority (FAA)] сообщило об интерференции с системами Доплеровского Метеорологического Радара [Terminal Doppler Weather Radar (TDWR)]. В результате, FCC вернула сертификацию устройств 802.11 в полосах U-NII-2 и U-NII-2E, которые требуют DFS. Сертификация в итоге была возобновлена; однаковы правила изменились, и сейчас радиомодули 802.11 могут передавать в частотном пространстве 5.60–5.65 ГГц, где работает TDWR. Каналы 120-128 долгие годы не были доступны. С Апреля 2014 года частотное пространство TDWR стало снова доступно для передач 802.11 в Соединенных Штатах.
18. A, B. OFDM использует модуляцию BPSK и QPSK для низких скоростей передачи данных OFDM. Более высокие скорости передачи данных OFDM используют модуляцию 16-QAM, 64-QAM, и 256-QAM. Модуляция QAM – это гибрид фазовой и амплитудной модуляции.
19. В. Когда биты данных конвертируются в серию битов, эти биты, которые представляют данные называются элементами или чипами [chips].
20. В. Для Wi-Fi связи вне помещений в полосах U-NII-5 и U-NII-7, FCC будет требовать использовать автоматизированную координацию частот [automated frequency coordination (AFC)], чтобы защитить существующие сервисы. Система AFC будет использовать базы данных геолокации, чтобы управлять назначением частот в реальном времени, чтобы защитить работу существующих устройств от радио интерференции.

## Глава 7: Топологии Беспроводных ЛВС

1. D, E. Идентификатор состава сервиса [service set identifier (SSID)] - это логическое имя из 32 символов, чувствительных к регистру, используемое для идентификации беспроводной сети 802.11. Идентификатор расширенного состава сервиса [extended service set identifier] - это логическое имя, используемое для расширенного состава сервиса [extended service set (ESS)]. ESSID часто является синонимом SSID.
2. В, D. Стандарт 802.11 определяет четыре состава сервиса, или топологии. Базовый состав сервиса [basic service set (BSS)] определяется как одна точка доступа (ТД) и

ассоциированные клиенты. Расширенный состав сервиса [extended service set (ESS)] определяется как один или более BSS соединенных средой системы распространения [distribution system medium (DSM)]. Независимый базовый состав сервиса [independent basic service set (IBSS)] не использует ТД и состоит исключительно из клиентских станций (STAs). Персональный базовый состав сервиса [personal basic service set (PBSS)], используемый радиомодулями 802.11ad, похож на IBSS, из-за отсутствия централизованной точки доступа в качестве портала в DSM.

3. F. По проекту, стандарт 802.11 не указывает среду для использования в системе распространения [distribution system (DS)]. Среда системы распространения [distribution system medium (DSM)] может быть Ethernet 802.3 магистралью, беспроводной средой или другой средой.
4. D. Беспроводная персональная вычислительная сеть [wireless personal area network (WPAN)] - это беспроводная топология на короткие расстояния. Bluetooth и Zigbee - это технологии, которые часто используются в WPANs.
5. A. В большинстве типовых применений расширенного состава сервиса [extended service set (ESS)] есть точки доступа (ТД) с перекрывающимися зонами покрытия. Цель в ESS с перекрывающимися зонами покрытия в бесшовном роуминге.
6. A, C, D. Размер и форма области базового сервиса [basic service area (BSA)] может зависеть от многих переменных, включая мощность передачи точки доступа (ТД), усиление антенны, и физическое окружение. Вы можете также поспорить, что фактическая форма и размер BSA в реальности зависит от точки зрения каждой подключенной клиентской станции, потому что все клиентские устройства по разному интерпретируют индикатор силы принятого сигнала (RSSI).
7. A, E. У каждой БЛВС есть логическое имя (SSID), и у каждого базового состава сервиса [basic service set (BSS)] есть уникальный идентификатор 2ого уровня (the BSSID). BSSID может быть физическим MAC адресом радиомодуля точки доступа; однако, можно создать несколько BSSID для радиоинтерфейса с помощью подинтерфейсов. Несколько BSSID обычно увеличивают значение исходного MAC адреса радиомодуля ТД. Множество производителей корпоративного Wi-Fi поддерживают передачу до 16 SSID и фактически 16 BSS с одного радиомодуля ТД. Однако, максимально число SSID и BSSID на радиомодуль зависит от производителя. Дополнительно, при создании нескольких SSID, существует несколько базовых составов сервиса [basic service sets (BSSs)], которые приводят к чрезмерному количеству избыточной служебной информации [overhaed] на MAC уровне. results in excessive amounts of MAC layer overhead.
8. B, E, F. Стандарт 802.11-2020 определяет независимы базовый состав сервиса [independent basic service set (IBSS)] как состав сервиса, использующий связь равный-с равным [peer-to-peer] без использования точки доступа (ТД). Другие названия для IBSS включают сеть "на лету" [ad hoc network] и одноранговая сеть [peer-to-peer network].
9. A, B, D. Клиенты, которые настроены в инфраструктурный режим, могут взаимодействовать через точку доступа (ТД) с другими беспроводными клиентскими станциями в пределях базового состава сервиса [basic service set (BSS)]. В обычном BSS, связи равный-с-равным [peer-to-peer] от одной клиентской станции до другой клиентской станции может происходить же тех пор, пока трафик пересыпается через ТД. Клиенты, которые поддерживают установку туннелированного прямого канала связи [tunneled direct link setup (TDLS)] являются редким исключением из этого правила. Клиенты с поддержкой TDLS могут связываться напрямую друг с другом, минуя ТД. Клиенты могут также связываться через ТД с другими сетевыми устройствами, которые присутствуют в среде системы распределения [distribution system medium (DSM)], например: сервер или настольное устройство. Интеграционный сервис ТД будет пересыпать полезную нагрузку блока данных MAC сервиса [MAC service data unit (MSDU)] от беспроводных клиентов 802.11 в кадры 802.3, когда DSM это Ethernet.

10. B, C, D, F. Топологии 802.11, или составы сервиса, определенные стандартом 802.11-2020 - это базовый состав сервиса [basic service set (BSS)], расширенный состав сервиса [extended service set (ESS)], независимый базовый состав сервиса [independent basic service set (IBSS)], персональный базовый состав сервиса [personal basic service set (PBSS)], базовый состав сервиса с поддержкой качества сервиса [QoS basic service set (QBSS)], и взаимосвязанный базовый состав сервиса [mesh basic service set (MBSS)]. DSSS и FHSS являются технологиями расширения спектра.
11. A. Беспроводная городская вычислительная сеть [wireless metropolitan area network (WMAN)] обеспечивает покрытие городской территории, такой как большой город и окружающий пригород.
12. D. Идентификатор базового состава сервиса [basic service set identifier (BSSID)] - это 48 битный (би- октетный) MAC адрес. MAC адреса существуют на MAC подуровне Канального уровня [Data-Link layer] модели OSI. BSSID - это идентификатор 2ого уровня базового состава сервиса [basic service set (BSS)].
13. B, C, E. Идентификатор базового состава сервиса [basic service set identifier (BSSID)] это идентификатор 2ого уровня или базового состава сервиса [basic service set (BSS)], или независимого базового состава сервиса [independent basic service set (IBSS)]. 48битный (би октетный) MAC адрес радиомодуля точки доступа - это BSSID внутри BSS. Топология расширенного состава сервиса [extended service set (ESS)] использует несколько ТД, таким образом существуют несколько BSSID. В сети IBSS, первая станция, которая включилась, генерирует случайным образом виртуальный BSSID в формате MAC адреса. FHSS и HR- DSSS являются технологиями расширения спектра.
14. D. Поправка 802.11s-2011, которая теперь является частью стандарта 802.11-2020, определяет новый состав сервиса для взаимосвязной топологии 802.11. Когда точки доступа (ТД) поддерживают функциональность взаимосвязываемости [mesh], они могут быть установлены там, где невозможен проводной доступ к сети. Функционал взаимосвязываемости используется для предоставления беспроводного распространения сетевого трафика, и набор ТД, которые предоставляют взаимосвязываемое [mesh] распространение формируют взаимосвязанный базовый состав сервиса [mesh basic service set (MBSS)].
15. D. Аналогично независимому базовому составу сервиса [independent basic service set (IBSS)], персональный базовый состав сервиса [personal basic service set (PBSS)] является топологией БЛВС 802.11, в которой станции 802.11ad взаимодействуют прямо друг с другом. PBSS может быть установлен только радиомодулями направленного мультигигабита [directional multi-gigabit (DMG)], которые передают в полосе частот 60 ГГц. Аналогично IBSS, там нет централизованной функции точки доступа, работающей в качестве портала в среду системы распространения [distribution system medium (DSM)].
16. A. Сервис станции [station service (SS)] присутствует во всех станция 802.11, включая клиентские станции и точки достпа (ТД). SS обеспечивает такие возможности, как аутентификация, деаутентификация, конфиденциальность данных, и т.д. Сервис системы распространения [distribution system service (DSS)] работает только в ТД и порталах взаимосвязности [mesh portals]. Сервис контрольной точки PBBS определен специально для радиомодулей 802.11ad при работе в очень специфичной топологии 802.11, называемой персональный базовый состав сервиса (PBSS) [personal basic service set (PBSS)]. Интеграционный сервис позволяет доставку блоков данных сервиса MAC [MAC service data units (MSDUs)] между системой распространения [distribution system (DS)] и не-IEEE-802.11 ЛВС через портал.
17. C. Расширенный состав сервиса [extended service set (ESS)] это два и более базовых состава сервиса [basic service sets (BSSs)] соединенных системой распространения [distribution system (DS)]. ESS - это набор нескольких точек доступа (ТД) и их ассоциированных клиентских

станций, объединенных единой средой системы распространения [distribution system medium (DSM)].

18. А. Беспроводная система распространения [wireless distribution system (WDS)] может подключить точки доступа (ТД), используя беспроводные транзитные каналы, при этом позволяя клиентам также ассоциироваться с радиомодулями точек доступа.
19. В. С. Система распространения [distribution system (DS)] состоит из двух основных компонентах. Среда системы распространения [distribution system medium (DSM)] является логической физической средой, используемой для подключения точек доступа (ТД). Сервис системы распространения [distribution system service (DSS)] располагается в станции ТД, и используется для управления ассоциациями, переассоциациями и деассоциациями клиентских станций.
20. В. Стандарт 802.11-2020 считается стандартом беспроводной локальной вычислительной сети (БЛВС) [wireless local area network (WLAN)].  
Оборудование 802.11 может, однако, быть использовано в других беспроводных топологиях.

## Глава 8: Доступ к Среде 802.11

1. В. Множественный Доступ с Контролем Несущей и Предотвращением Конфликтов [Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)] – это способ контроля доступа к беспроводной среде, который являются частью Функции Распределенной Координации [Distributed Coordination Function (DCF)]. Множественный Доступ с Контролем Несущей и Обнаружением Конфликтов [Carrier Sense Multiple Access with Collision Detection (CSMA/CD)] используется в 802.3, а не в 802.11. Передача жетонов [Token passing] используется в сетях Token Ring и Fiber-Distributed Data Interface (FDDI). Запрашиваемый приоритет [Demand priority] используется в сетях 100BaseVG.
2. Е. Технология 802.11 не использует обнаружение конфликтов (коллизий). Если кадр подтверждения (ACK) не получен исходным передающим радиомодулем, то односторонний [unicast] кадр не подтвержден и должен быть передан повторно. Этот процесс не определяет конкретно произошел ли конфликт. Ошибка в получении кадра ACK от приемника означает, что или односторонний [unicast] кадр не был доставлен станции назначения, или кадр ACK не был получен, но нельзя положительно определить причину. Это может быть из-за конфликта (коллизии) или других причин, таких как высокий уровень шума. Все другие варианты используются, чтобы помочь предотвратить конфликты.
3. Д. Кадры подтверждения (ACK) и кадры чисто-для- отправки или готов-к-приему [clear-to-send (CTS)] следуют за коротким межкадровым пространством [short interframe space (SIFS)].
4. Д, Е. Таймер вектора распределения сети [network allocation vector (NAV)] управляет прогнозом будущего трафика в среде на основе информации значения длительности, которую видно в предыдущем кадре передачи. Виртуальный контроль несущей использует NAV, чтобы определить доступность среды. Физический контроль несущей проверяет радиоволновую среду на доступность несущей. Физический контроль несущей происходит во время оценки чистоты канала [clear channel assessment (CCA)]. Окно конкурентной борьбы [contention window] и таймер обратного отсчета [backoff timer] являются частью процедуры псевдослучайного обратного отсчета [pseudo-random backoff]. Окна контроля канала не существует.
5. С. Первый шаг – это выбор случайного значения отсрочки. После того как значение выбрано, оно умножается на время слота. Таймер случайной отсрочки затем начинает обратный отсчет

**1000 Приложение А • Ответы на Контрольные Вопросы**

числа времени слота. Когда число достигнет нуля, станция может начать передачу.

6. В, D. Радиомодули 802.11 используют два отдельных порога оценки чистоты канала [clear channel assessment (CCA)] когда слушает радиоволновую среду. Порог обнаружения сигнала [signal detect (SD)] используется для идентификации каждой преамбулы передачи 802.11 от другого передающего радиомодуля 802.11. Порог обнаружения энергии [energy detect (ED)] используется для обнаружения любого другого типа радиопередачи во время оценки чистоты канала [clear channel assessment (CCA)].
7. В, D. Поле Длительность/ID [Duration/ID] используется для установки вектора распределения сети [network allocation vector (NAV)], который является частью процесса виртуального контроля несущей. Окно конкурентной борьбы и случайный таймер отсрочки являются частью процесса отсрочки, который производится после процесса контроля несущей.
8. D. Цель справедливости эфирного времени в выделении равного времени против равных возможностей. Справедливость доступа [Access fairness] и гибкий доступ к среде [opportunistic medium access] не существуют. Множественный Доступ с Контролем Несущей и Предотвращением Конфликтов [Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)] является обычным режимом контроля доступа к среде для Wi-Fi устройств.
9. A, B, D, E. Функция Распределенной Координации [Distributed Coordination Function (DCF)] определяет четыре проверки и баланса Множественного Доступа с Контролем Несущей и Предотвращением Конфликтов [Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)], чтобы гарантировать, что только один радиомодуль 802.11 передает в полу duplexной среде. Виртуальный контроль несущей, физический контроль несущей, межкадровое пространство, и случайный таймер отсрочки работают все вместе. Обнаружение конфликтов не является частью CSMA/CA.
10. В. На текущий момент, Wi-Fi Мультимедиа (WMM) основана на механизмах Расширенного Распределенного Доступа к Каналам [Enhanced Distributed Channel Access (EDCA)], определенного поправкой 802.11e, которая теперь является частью стандарта 802.11-2020. Сертификация WMM обеспечивает приоритезацию трафика по четырем категориям доступа. EDCA – это подфункция Функции Гибридной Координации [Hybrid Coordination Function (HCF)]. Другая подфункция HCF – это Доступ к Каналу, Контролируемый Функцией Гибридной Координации [Hybrid Coordination Function Controlled Channel Access (HCCA)].
11. Е. Функция Гибридной Координации [Hybrid Coordination Function (HCF)] определяет способность радиомодуля 802.11 посыпать несколько кадров при передаче в радиосреду. Когда HCF-совместимый радиомодуль борется за среду, он получает определенное количество времени для отправки кадров, которое называется возможность передачи [transmit opportunity (TXOP)]. Во время TXOP, радиомодуль 802.11 может послать один кадр или несколько кадров. Во время TXOP, несколько кадров могут быть отправлены, используя механизм агрегации кадров, или может быть отправлена серия кадров [frame burst].
12. А, B, D, E. Приоритет WMM Аудио [WMM Audio] не существует. Сертификация Wi-Fi Мультимедиа [Multimedia (WMM)] обеспечивает приоритезацию трафика по четырем категориям доступа: Голос [Voice], Видео [Video], Обычные или Без гарантированной доставки данные [Best Effort] и Фоновые данные [Background].
13. С. Вся суть Wi-Fi Мультимедиа [Wi-Fi Multimedia (WMM)] в приоритезации разных классов трафика приложений во время процесса борьбы за среду. Трафик в голосовой категории доступа имеет лучшие шансы при борьбе за среду во время процесса отсрочки [backoff process]. Для голосового трафика требуется минимальное время ожидания короткого межкарового пространства [short interframe space (SIFS)] плюс два слота, а затем

окно конкурентной борьбы 0-3 слота прежде чем передавать в среду. Негарантированный [Best-effort] трафик должен ждать минимальное время SIFS и три слота, затем окно конкурентной борьбы 0-15 слотов. Процесс борьбы все еще полностью псевдо-случайный; однако, шансы у голосового трафика лучше..**14.** В. Метод доступа к середе - Расширенный Распределенный Доступ к Каналу обеспечивает

приоритезацию трафика через использование меток приоритета [priority tags] 802.1D. Метки приоритета 802.1D предоставляют механизм для внедрения качества сервиса [quality of service (QoS)] на MAC уровне. Доступны разные классы сервиса, представляемые 3мя битами поля [user priority] пользовательский приоритет в заголовке IEEE 802.1Q, добавленному к Ethernet кадру. Метки приоритета 802.1D [802.1D priority tags] со стороны Ethernet используются для направления трафика по разным очередям категории доступа.

- 15.** А, Е. Первая задача – определить является ли передача кадра входящей для станции, чтобы начать прием. Если среда занята, радиомодуль попытается синхронизоваться с передачей. Вторая задача в определении занята ли среда перед передачей. То называется оценкой чистоты канала [clear channel assessment (CCA)]. ССА включает прослушивание радиопередач 802.11 на Физическом уровне. Среда должна быть чистой прежде, чем станция сможет передавать.
- 16.** В. Порог обнаружения сигнала [signal detect (SD)] используется для идентификации каждой преамбулы 802.11 передачи от другого предающего радиомодуля 802.11. Преамбула – это компонента заголовка Физического уровня передачи кадра 802.11. Преамбула используется для синхронизации между передающим и принимающим радиомодулями 802.11. Порог SD иногда называется, как порог обнаружения (контроля) преамбулы несущей. Порог SD статистически где-то около 4 dB отношения сигнал-шум [signal-to-noise ratio (SNR)] для большинства радиомодулей 802.11 для обнаружения и декодирования преамбулы 802.11.
- 17.** С. Когда слушающий радиомодуль слышит передачу кадра другой станции, он смотрит заголовок кадра и определяет содержит ли поле Длительность/ID [Duration/ID] значение Длительности или значение ID. Если поле содержит значение Длительности [Duration], то слушающая станция установит свой таймер вектора распределения сети [network allocation vector (NAV)] в это значение. Значение длительности в каждом кадре – то количество времени после того, как кадр получен, которое нужно, чтобы завершить обмен оставшимися кадрами между двумя радиомодулями.
- 18.** В. Расширенный Распределенный Доступ к Каналам [Enhanced Distributed Channel Access (EDCA)] предоставляет дифференцированный доступ для станций с помощью четырех категорий доступа. Метод доступа к среде EDCA предоставляет для приоритезации трафика по четырем категориям доступа, которые соответствуют восьми меткам приоритета 802.1D [802.1D priority tags].
- 19.** А. Подтверждения (ACKs) используются для подтверждения [verification] доставки однокапельных [unicast] кадров 802.11. Широковещательные [Broadcast] и многокапельные [multicast] кадры не требуют подтверждения. Кадров Anycast не существует.
- 20.** А, Д. Станция 802.11 может бороться за среду в течении окна времени, которое называется, как время отсрочки [backoff time]. В этой точке в процессе Множественного Доступа с Контролем Несущей и Предотвращением Конфликтов [Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)] станция выбирает случайное значение отсрочки с помощью псевдо-случайного алгоритма отсрочки [pseudo-random backoff algorithm]. Станция выбирает случайное число из диапазона, который называется значением окна конкурентной борьбы [contention window (CW)]. После того, как случайное число выбрано, число умножается на значение времени слота. Это запускает псевдо-случайный таймер отсрочки (обратного отсчета). Не перепутайте таймер отсрочки с таймером NAV. Таймер NAV – это механизм виртуального контроля несущей [virtual carrier sense], используемый для резервирования среды для дальнейшей передачи. Псевдо-случайный таймер отсрочки

[pseudo-random backoff timer] – это финальный таймер, используемый станцией перед передачей.

## Глава 9: 802.11 MAC

1. С. Только кадры данных 802.11 могут переносить полезную нагрузку более высоких уровней (MSDU) в теле кадра. MSDU может быть 2304 байта, и обычно шифруется. У 802.11 кадров контроля нет тела. У 802.11 кадров управления есть тело; однако, полезная нагрузка кадра – это строго информация 2ого уровня. Кадр действия – это подтип кадров контроля 802.11. Кадры запроса на ассоциацию и ответов на запрос на ассоциацию являются подтипаами кадров управления 802.11.
2. D. IP пакет состоит из информации уровней 3–7. Блок данных MAC сервиса [MAC service data unit (MSDU)] состоит из данных подуровня LLC и/или любого количества уровней выше Канального [Data-Link] уровня. MSDU – это полезная нагрузка, находящаяся внутри тела кадра данных 802.11.
3. E. Этот экран перехвата заголовка 802.11 показывает четыре MAC адреса. Хотя у кадров 802.11 четыре адресных поля в заголовке MAC, обычно кадры 802.11 используют только три поля MAC адресов. Кадр 802.11, посланный внутри беспроводной системы распространения [wireless distribution system (WDS)], требует все четыре MAC адреса. Хотя стандарт конкретно не определяет процедуру использования того формата, производители БЛВС часто применяют решение WDS. Пример WDS – это канал БЛВС точка-точка типа мост. Еще один пример WDS – это взаимосвязанная транзитная связь между ТД взаимосвязанным [mesh] порталом и ТД взаимосвязанными [mesh] точками.
4. A, C, D. Сигналы ERP ТД для использования механизма защиты в информационном элементе ERP в кадре маяка. Если не-ERP [non-ERP] STA ассоциирована с ТД ERP, ERP ТД включает NonERP\_Present бит в свои маяки, включая механизм защиты в своем BSS. Другими словами, ассоциация клиента HR-DSSS (802.11b) запустит защиту. Если ТД ERP слышит маяк только с 802.11b или набор поддерживаемых скоростей 802.11 от другой ТД или IBSS STA, она включает бит NonERP\_Present в своих собственных маяках, включая механизмы защиты в своем BSS.
5. A, B, C, D. Кадр зондирующего ответа [probe response frame] содержит ту же самую информацию, что и кадр маяк, за исключением карты индикации наличия трафика [traffic indication map].
6. B, D. Маяки не могут быть выключены. Клиенты используют информацию временных отметок из маяков, чтобы синхронизоваться с другими станциями на беспроводной сети. Только ТД посылают маяки в BSS; клиентские станции посылают маяки в IBSS. Маяки могут содержать проприетарную информацию.
7. A, D. В зависимости от того, как используются поля To DS и From DS, определение четырех полей MAC адресов изменится. Одно постоянно, однако, то то, что поле Адрес 1 [Address 1] всегда будет адресом приемника [receiver address (RA)], но может иметь и второе определение тоже. Поле Адрес 2 [Address 2] всегда будет адресом передатчика [transmitter address (TA)], но также может иметь второе определение. Адрес 3 [Address 3] обычно используется для информации о дополнительном MAC адресе. Адрес 4 используется только в случае WDS.
8. D. Когда отправлен кадр RTS, значение поля Длительность/ID [Duration/ID] равно времени, необходимому для передачи кадров CTS, Данных, и подтверждений [ACK], плюс три интервала SIFS.

9. В. Когда клиентская станция передает кадр с полем Управление Питанием [Power Management], установленным в 1, включается режим сбережения энергии [power-save mode]; он только уведомляет клиентов оставаться «бодрыми» при подготовке к мультикасту [multicast] или широковещанию [broadcast].
10. А, В. Принимающая станция может получить данные, но возвращаемый кадр ACK может быть поврежден, и исходный однокапельный [unicast] кадр должен быть передан повторно. Если однокапельный [unicast] кадр поврежден по любой причине, принимающая станция не отправит ACK.
11. В. Кадр PS-Poll используется станцией, чтобы запросить закэшированные данные. ATIM используется, чтобы оповестить станции к IBSS о закэшированных данных. Бит Управления Питанием [Power Management] используется станцией для уведомления ТД о том, что станция собирается перейти в режим энергосбережения [power-save mode]. DTIM используется для того, чтобы показать клиентской станции как часто просыпаться, чтобы получить забуферизированные широковещательные [broadcast] и многонаправленные [multicast] кадры. Карта индикации наличия трафика [traffic indication map (TIM)] – это поле в кадре маяка, используемой ТД для того, чтобы показать, что есть забуферизированные однокапельные [unicast] кадры для клиентов в режиме энергосбережения.
12. А, Е. Все радиомодули ТД 802.11 будут отправлять зондирующий ответ [probe response] на направленные кадры зондирующего запроса [probe request], которые содержат корректное значение SSID. ТД должна также ответить на кадры пустого зондирующего запроса [null probe request], которые содержат пустое значение SSID. Некоторые производители предлагают возможность отвечать на пустые зондирующие запросы [null probe requests] пустым зондирующими ответом [null probe response]. Радиомодуль ТД 802.11ac будет отвечать клиентским станциям 802.11ac также как клиентским станциям 802.11a/n передающим зондирующие запросы [probe requests] на 5 ГГц. Как и все кадры управления, зондирующие запросы не зашифрованы. Бит Управления Питанием [Power Management] используется клиентом, чтобы показать клиентское состояние энергопотребления.
13. А, Д. Существует два типа сканирования: пассивное, которое происходит, когда станция слушает маяки, чтобы обнаружить ТД, и активное, которое происходит, когда станция отправляет зондирующие запросы [probe requests] в поисках ТД. Станции отправляют зондирующие запросы только, если они производят активное сканирование. После того, как станция ассоциировалась, является обычным для станции продолжать изучать наличие ближайших ТД. Все клиентские станции поддерживают список “известных ТД”, который постоянно обновляется активным сканированием.
14. В, Д, Е. Хотя существуют схожести, адресация, используемая MAC кадрами 802.11 намного более сложная, чем кадров Ethernet. У кадров 802.3 есть только адрес источника [source address (SA)] и адрес назначения [destination address (DA)] в заголовке 2ого уровня. Четыре MAC адреса, используемые кадром 802.11, могут быть использованы как пять различных типов адресов: адрес приемника [receiver address (RA)], адрес передатчика [transmitter address (TA)], идентификатор базового состава сервиса [basic service set identifier (BSSID)], адрес назначения [destination address (DA)], и адрес источника [source address (SA)].
15. В. Когда клиент впервые пытается подключиться к ТД, он сначала отправит зондирующий запрос [probe request], и слушает в ожидании зондирующего ответа [probe response]. После того, как он получил ответ на зондирующий запрос [probe response], он попытается аутентифицироваться с ТД, а затем ассоциироваться (т.е. соединиться) с сетью.

**1004 Приложение А • Ответы на Контрольные Вопросы**

- 16.** В. Карта индикации доставки трафика [delivery traffic indication map (DTIM)] используется, чтобы гарантировать, что все станции, использующие управление питанием [power management] находятся в активном режиме, когда посыпается многонаправленный [multicast] или широковещательный [broadcast] трафик. Интервал DTIM важен для всех приложений, которые используют многовещание [multicasting]. Например, многие производители VoWiFi поддерживают функции нажми-чтобы-говорить [push-to-talk], чтобы отправить VoIP трафик на мультикастный адрес [multicast address]. Неправильно настроенный интервал DTIM может вызвать проблемы с производительностью во время многоадресного вещания [multicast] нажми-чтобы-говорить [push-to-talk].
- 17.** А, С. ТД 802.11n/g обратно совместима с 802.11b и поддерживает скорости передачи данных HR-DSSS 1, 2, 5.5, и 11 Мбит/с, а также скорости передачи данных ERP-OFDM в 6, 9, 12, 18, 24, 36, 48, и 54 Мбит/с. Если администратор БЛВС выключил скорости передачи данных 1, 2, 5.5, и 11 Мбит/с, обратная совместимость фактически выключается, и клиенты 802.11b не смогут подключиться. Стандарт 802.11-2020 определяет использование базовых скоростей, которые являются требуемыми скоростями. Если клиентская станция не поддерживают любую из базовых скоростей, используемую ТД, клиентской станций будет отказано в ассоциации с BSS. Если администратор БЛВС настроил скорости передачи данных ERP- OFDM 6 и 9 Мбит/с в качестве базовых скоростей, клиентам 802.11b (HR-DSSS) будет отказано в ассоциации, потому что они не поддерживают эти скорости.
- 18.** А, В. Некоторые кадры данных 802.11 в действительности не несут никаких данных. Кадры Null и QoS Null являются кадрами не несущими данные [non-data-carrying frames]. У кадров данных 802.11 есть заголовок и окончание, но нет тела кадра, которое переносит полезную нагрузку MSDU. Эти кадры иногда называют как кадры с нулевым действием [null function frames], потому что полезная нагрузка - пустая, и тем не менее кадр все еще выполняет свою задачу.
- 19.** В, Д. Кадр действия [action frame] - это тип кадра управления, используемый для запуска определенных действий в BSS. Кадры действия могут быть отправлены точками доступа или клиентскими станциями. Кадр действия предоставляет информацию и направление относительного того, что делать. Кадр действия иногда называется, как "кадр действия, который может делать всё". Полный список всех текущих кадров действия можно найти в разделе 9.6 стандарта 802.11-2020. Один пример того, как используются кадры действия - это оповещение о смене канала [channel switch announcement (CSA)] от ТД, передающей на канале динамического выбора частоты [dynamic frequency selection (DFS)]. Еще один пример кадра действия - это запрос и ответ отчета о соседях [neighbor report], который могут использовать 802.11k совместимые радиомодули. Информация отчета о соседях используется клиентскими станциями для получения информации от ассоциированной ТД о потенциальных соседях для роуминга.
- 20.** А, F. Поле Повторная Передача или Повтор [Retry] со значением 1, означает, что это повторная передача. Каждый раз когда радиомодуль 802.11 передает однонаправленный [unicast] кадр, если кадр получен надлежащим образом, и прошла проверка циклической избыточности [cyclic redundancy check (CRC)] FCS, то радиомодуль 802.11, который принял кадр, ответит кадром подтверждения [acknowledgment (ACK)]. Если ACK получен, исходная станция знает, что кадр был успешно передан. Все однонаправленные [unicast] кадры 802.11 должны быть подтверждены. Широковещательные [Broadcast] и Многонаправленные [multicast] кадры не требуют подтверждения. Если любая часть однонаправленного кадра повреждена, CRC не пройдет, и приемный радиомодуль 802.11 не отправит кадр ACK передающему радиомодулю 802.11. Если кадр ACK не получен исходным передающим радиомодулем, однонаправленный [unicast] кадр не подтвержден, и должен быть отправлен повторно.

# Глава 10: Технология MIMO: HT и VHT

1. A, D, E. Поправка 802.11ac поддерживает BPSK, QPSK, 16-QAM, 64-QAM, и 256-QAM. 1024-QAM поддерживается только устройствами 802.11ax. BASK не существует.
2. A, C, D. Пространственное мультиплексирование передает несколько потоков уникальных данных в одно и то же время. Если точка доступа MIMO посыпает два уникальных потока данных клиенту MIMO, который получает оба потока, пропускная способность фактически удваивается. Если точка доступа MIMO посыпает три уникальных потока данных клиенту MIMO, который принимает все три потока, пропускная способность фактически утраивается. Поскольку формирование луча передачи [transmit beamforming] приводит к конструктивной связи с многолучевым распространением [multipath], то в результате получаем более высокое отношение сигнал-шум и более высокую амплитуду на приеме. Формирование луча передачи [Transmit beamforming] приведет к более высокой пропускной способности, потому что более высокое SNR позволяет использовать более сложные методы модуляции, которые могут закодировать больше битов данных. 40 МГц HT каналы фактически удваивают ширину полосы частот, что приводит к большей пропускной способности. A-MPDU -это не технология Физического уровня [Physical layer].
3. D. Энергосбережение в пространственном мультиплексировании [Spatial multiplexing power save (SM power save)] позволяет устройствам 802.11n MIMO выключать все радиомодули кроме одного. Например, устройство 4×4 MIMO с четырьмя радиоцепями отключило бы три из четырех радиомодулей, сберегая таким образом энергию. Энергосбережение в пространственном мультиплексировании [SM power save] определяет два метода работы: статический и динамический.
4. E. Защитный интервал действует как буфер для разброса задержки [delay spread], а нормальный защитный интервал - это 800-наносекундный буфер между символными передачами. Защитный интервал компенсирует разброс задержки [delay spread] и помогает предотвратить межсимвольную интерференцию. Если защитный интервал слишком короткий, будет происходить межсимвольная интерференция. У радиомодулей HT/VHT также есть возможность использования короткого 400-наносекундного защитного интервала [GI].
5. A, B, C, D, E. Все они являются поддерживаемыми ширинами каналов. Канал 160 МГц в действительности состоит из двух 80 МГц каналов, которые могут быть соседними или разделены.
6. A, B, D. Поправка 802.11n представила два новых метода агрегации кадров, чтобы помочь уменьшить служебную информацию [overhead] и увеличить пропускную способность. Агрегация кадров - это метод объединения нескольких кадров в одну передачу кадра. Существует два типа агрегации кадров - A-MSDU и A-MPDU. Кадры Блокового подтверждения [Block ACK] используются для подтверждения A-MPDUs. Защитный интервал и пространственное мультиплексирование используются на Физическом уровне.
7. B, D, E. Формирователь луча [beamformer] передает кадр оповещения NDP, за которым следует кадр NDP. Получатель луча [beamformee] обрабатывает эту информацию и создает и передает матрицу обратной связи [feedback matrix]. ТД использует матрицы обратной связи [feedback matrices], чтобы вычислить управляющую матрицу [steering matrix], которая используется для направления передачи.

8. А. Радиомодули MIMO передают несколько радиосигналов в одно и то же время, и используют с выгодой многолучевое распространение [multipath]. Каждый индивидуальный радиосигнал передается уникальным радиомодулем и антенной MIMO системы. Каждый независимый сигнал называется, как пространственный поток [spatial stream], а каждый поток может содержать отличные от других потоков данные, переданные одним или более другими радиомодулями. Система MIMO 3×3:2 может передавать два уникальных потока данных. Система MIMO 3×3:2 использует три передатчика и три приемника; однако, два уникальных потока могут быть использованы.
9. А. Несколько MPDUs могут быть агрегированы в один кадр. Отдельные MPDUs внутри одного A-MPDU должны все иметь один и тот же адрес приемника [receiver address]. Однако, отдельные MPDUs должны все быть одной и той же категории доступа качества сервиса [quality-of-service access category] 802.11e. Каждый агрегированный MPDU также шифруется и дешифруется независимо.
10. Д. Режимы 0, 1, и 2, все определяют защиту для использования в разных ситуациях, где только станциям 802.11n/ac разрешено ассоциироваться с точкой доступа 802.11n/ac. Режим 3 - Не-HT Смешанный Режим [Mode 3—Non-HT Mixed mode]—определяет использование защиты, когда радиомодули и HT/VHT, и non-HT ассоциированы с точкой доступа 802.11ac.
11. А, В, Е. Каждый 40 МГц канал состоит из первичного [primary] и вторичного [secondary] 20 МГц каналов. Первичный и вторичный 20 МГц каналы должны быть смежными 20 МГц каналами на частоте в которой они работают. Первичный и вторичный каналы используются вместе только для передачи кадров данных между ТД 802.11n/ac и клиентом 802.11n/ac. Для обратной совместимости, все кадры управления и контроля 802.11 передаются только на первичном [primary] канале. Кроме того, только первичный канал используется для передачи данных между ТД 802.11n/ac и устаревшими клиентами 802.11a/g.
12. С, D, Е. Разнесение с циклическим сдвигом [Cyclic shift diversity (CSD)], пространственно-временное блочное кодирование [space-time block coding (STBC)], и пространственное мультиплексирование [spatial multiplexing (SM)] являются методами разнесения по передаче MIMO. STBC и SM требуют радиомодули MIMO на обоих сторонах канала связи. В отличие от STBC и SM, сигнал от передатчика MIMO, который использует CSD, может быть принят устаревшими устройствами 802.11g и 802.11a. Комбинация максимального отношения [Maximal ratio combining (MRC)] - это техника разнесения по приему. DSSS - это технология расширения спектра, используемая устаревшими радиомодулями 802.11 SISO.
13. А, В, D. Радиомодули 802.11n (HT) обратно совместимы с более старыми радиомодулями 802.11b (HR- DSSS), 802.11a (OFDM), и 802.11g(ERP). Радиомодули HT обратно не совместимы с устаревшими радиомодулями с перестройкой частоты.
14. В. 802.11ac определяет только 10 MCSs, в отличие от 802.11n, которая определяет 77. 802.11n определяет MCSs на основе модуляции, методов кодирования, числа пространственных потоков, размеров канала и защитного интервала. 802.11ac определяет 10 MCSs на основе модуляции и скоростей(индекса) кодирования.
15. D. MCS 0–7 являются обязательными. MCS 8 и MCS 9 используют 256-QAM, который является опциональным, но скорее всего поддерживается большинством производителей.
16. С. Разворачивание 40 МГц каналов в полосе 2.4 ГГц не масштабируется, потому что не достаточно частотного пространства. Хотя в 2.4 ГГц доступно 14 каналов, существует только три неперекрывающихся 20 МГц канала, доступных в полосе ISM 2.4 ГГц. Когда небольшие

каналы объединяются вместе, чтобы сформировать 40 МГц канал в полосе ISM 2.4 ГГц, любые два 40 МГц канала будут перекрываться. Модель переиспользования каналов невозможна для 40 МГц каналов в полосе ISM 2.4 ГГц. Полосы 5 ГГц имеют намного больше частотного пространства, следовательно, модель переиспользования 40 МГц каналов возможна с тщательным планированием.

17. В, Д. Радиомодули 802.11ac (VHT) обратно совместимы со всеми предыдущими совместимыми с 5 ГГц радиомодулями. Это включает радиомодули 802.11a (OFDM) и 5ГГц радиомодули 802.11n (HT).
18. В. Когда используется MIMO с разнесением по приему, сигнал может также быть линейно объединен (скомбинирован) с помощью техники обработки сигнала с названием комбинация максимальных отношений [ maximal ratio combining (MRC) ]. Алгоритмы используются для комбинации нескольких принятых сигналов путем анализа каждого уникального сигнала и оптимального комбинирования сигналов в метод, который является аддитивным, а не разрушительным. Системы MIMO, использующие MRC, фактически поднимают уровень SNR принимаемого сигнала. MRC также полезны, когда устаревший SISO радиомодуль передает MIMO приемнику и происходит многолучевое распространение [ multipath occurs ].
19. В. Радиомодули 802.11n/ac могут использовать 800-наносекундный защитный интервал; однако, более коротки 400-наносекундный защитный интервал также доступен. Более короткий защитный интервал ведет к более короткому символьному времени, что имеет эффект увеличения скорости передачи данных на 10 процентов. Если опциональный коротки 400-наносекундный защитный интервал используется в радиомодуле 802.11n, пропускная способность должна увеличиться. Однако, если происходит межсимвольная интерференция из-за многолучевого распространения, то будет повреждение данных. Если произошло повреждение данных, то увеличиваются повторные передачи на 2ом уровне и пропускная способность неблагоприятно пострадает. Следовательно, 400 наносекундный защитный интервал следует использовать только в хорошей радиосреде. Если пропускная способность упала из-за настройки короткого защитного интервала [GI], то нужно использовать заводской настройки защитного интервала в 800 наносекунд.
20. С. Поправка 802.11ac определяет максимум четыре пространственных потока для клиента и восемь пространственных потоков для ТД. Однако, большинство корпоративных ТД 802.11ac являются 4×4:4, а большинство клиентов 802.11ac являются 2×2:2.

## Глава 11: Архитектура БЛВС

1. А, Е. В централизованной архитектуре БЛВС автономные точки доступа (ТД) заменяются на точки доступа, контролируемые контроллером. Все три логические плоскости работы находятся внутри центрального сетевого устройства - контроллера БЛВС [WLAN controller]. Фактически, все плоскости перемещаются из точек доступа в контроллер БЛВС. Следует отметить, что система управления сетью [network management system (NMS)] может использоваться для управления контроллерами и ТД, управляемыми контроллерами.
2. Д. Телекоммуникационные сети часто определяются как три логические плоскости работы. Плоскость контроля состоит из контроля или сигнальной информации, и часто определяется как интеллект сети или протоколы.
3. А, С. Все три инфраструктуры БЛВС спроектированы, чтобы поддерживать использование виртуальных ЛВС [virtual LANs (VLANs)] и разметку 802.1Q [802.1Q tagging]. Однако, централизованная архитектура БЛВС обычно инкапсулирует пользовательские VLANы

между ТД, только управляемой контроллером, и контроллером БЛВС; следовательно, обычно требуется только один VLAN на границе. Транк 802.1Q, однако, обычно требуется между контроллером БЛВС и коммутатором ядра. Ни автономная, ни распределенной архитектуры БЛВС не используют контроллер. Безконтроллерная архитектура [Noncontroller architectures] требует поддержку разметки 802.1Q [802.1Q tagging], если поддерживаются несколько VLAN на границе сети. Точка доступа подключается к транковому 802.1Q порту пограничного коммутатора, который поддерживает разметку по VLANам [VLAN tagging].

4. В. Точки доступа, управляемые только контроллером, обычно пересылают пользовательский трафик центральному БЛВС контроллеру через инкапсулированный IP туннель. Автономные и совместноработающие [cooperative] точки доступа, обычно, используют локальную пересылку данных. Хотя весь смысл совместноработающей [cooperative] и распределенной модели БЛВС в устранении центральной пересылки пользовательского трафика в ядро, точки доступа могут также обладать возможностями IP туннелирования.
5. А, В, С. Множество производителей БЛВС используют Универсальную Маршрутизируемую Инкапсуляцию [Generic Routing Encapsulation (GRE)], которая наиболее популярный протокол сетевого туннелирования. Хотя GRE часто используется для инкапсуляции IP пакетов, GRE также может использоваться для инкапсуляции кадров 802.11 внутри IP туннеля. GRE туннель создает виртуальный канал связи точка-точка между точкой доступа, управляемой только контроллером, и контроллером БЛВС. Производители БЛВС, которые не используют GRE, используют проприетарные протоколы для IP туннелирования. Протокол управления - Контроль и Обеспечение Беспроводных Точек Доступа [Control and Provisioning of Wireless Access Points (CAPWAP)] также может использоваться для туннелирования пользовательского трафика. IPsec также может использоваться для безопасного туннелирования пользовательского трафика от ТД через канал WAN.
6. Д. Главный недостаток использования традиционной автономной точки доступа (ТД) в том, что нет центральной точки управления. Любая автономная архитектура БЛВС с 25ю или более точками доступа требует определенного рода систему управления сетью [network management system (NMS)]. Хотя контроллер БЛВС может быть использован для управления БЛВС в централизованной архитектуре БЛВС, но если развернуто несколько контроллеров, то может понадобиться NMS, чтобы управлять несколькими контроллерами. Хотя плоскость контроля и плоскость данных вернулись обратно на ТД в распределенной архитектуре БЛВС, плоскость управления осталась централизованной. Настройка и мониторинг за всеми точками доступа в распределенной модели все еще управляется NMS. Большинство решений NMS теперь являются облачными решениями управления.
7. Е. Основные производители контроллеров БЛВС внедрили, так называемую архитектуру разделения функций контроля доступа к среде [split MAC architecture]. В этом типе архитектуры БЛВС, некоторые сервисы контроля доступа к среде [MAC] управляются контроллером БЛВС, а некоторые управляются ТД, управляемыми только контроллером.
8. А, С, Е. Телефоны VoWiFi являются клиентскими станциями 802.11, которые работают через большинство архитектур БЛВС. Автоматической Телефонной Станции (АТС) [private branch exchange (PBX)] необходимо осуществлять соединения между внутренними телефонами частной компании, а также соединять их с Телефонной Сетью Общего Пользования [public switched tele- phone network (PSTN)] через транковые линии. Функционал качества сервиса Wi-Fi Мультимедиа [Wi-Fi Multimedia (WMM)] должен поддерживаться и VoWiFi телефоном и инфраструктурой БЛВС. На текущий момент

большинство решений Голос поверх Wi-Fi [Voice over Wi-Fi (VoWiFi)] используют Протокол Инициации Сеанса [Session Initiation Protocol (SIP)] в качестве протокола сигнализации для голосовой связи поверх IP сети, но могут быть использованы и другие протоколы.

9. Д. Централизованная пересылка данных - это традиционный метод пересылки данных, используемый контроллерами БЛВС. Весь пользовательский трафик 802.11 пересыпается от точки доступа (ТД) на контроллер БЛВС для обработки, особенно, когда контроллер БЛВС управляет шифрованием и дешифрованием, или применяет политики безопасности и качества сервиса (QoS). Большинство решений контроллеров БЛВС также теперь поддерживает распределенную плоскость данных. ТД, управляемые только контроллером, выполняют пересылку данных локально; они могут быть использованы в ситуациях, где лучше производить пересылку на границе, и избегать пересылку в центральную локацию сети для всех данных.
10. D, E. Распределенное решение, использующее корпоративного уровня маршрутизаторы БЛВС, часто устанавливаются в офисах филиалов компаний. У маршрутизаторов БЛВС филиалов есть возможность подключаться к корпоративной штаб-квартире с помощью туннелей виртуальной частной сети [virtual private network (VPN)] с помощью встроенного VPN клиента. У корпоративных маршрутизаторов БЛВС также есть встроенные межсетевые экраны [firewalls] с поддержкой проброса портов [port forwarding], трансляцией сетевого адреса [network address translation (NAT)], и трансляцией порта [port address translation (PAT)]. Корпоративные маршрутизаторы БЛВС также предлагают полную поддержку безопасности 802.11.
11. G. Стандарт 802.11 не указывает строго, какой тип форм фактора [form factor] должен быть использован радиомодулем 802.11. Хотя клиентские адаптеры PCMCIA и Mini PCI являются наиболее типовыми, радиомодули 802.11 существуют во множестве других форматах таких, как карты CompactFlash, карты Secure Digital, USB донглы, ExpressCards, и другие проприетарные форматы.
12. G. Все эти протоколы могут быть использованы для настройки устройств БЛВС, таких как точки доступа и контроллеры БЛВС. Однако, написанные корпоративные политики должны жестко предписывать использование безопасных протоколов, таких как SNMPv3, SSH2, и HTTPS.
13. F. Контроллеры БЛВС поддерживают функциональность роуминга на Земле уровне, политики распределения полосы [bandwidth policies], и инспекцию пакетов с учетом состояний [stateful packet inspection]. Адаптивное радио [Adaptive RF], мониторинг устройств [device monitoring], и управление ТД также поддерживается на контроллере.
14. C, E. Связь между сервером системы управления сетью [network management system (NMS)] и точкой доступа (ТД) требует протоколов управления и мониторинга. Большинство решений NMS использует Простой Протокол Сетевого Управления [Simple Network Management Protocol (SNMP)], чтобы управлять и мониторить БЛВС. Другие решения NMS также используют Контроль и Обеспечение Беспроводных Точек Доступа [Control and Provisioning of Wireless Access Points (CAPWAP)] строго в качестве протокола мониторинга и управления. CAPWAP включает в себя Безопасность Датаграм Транспортного Уровня [Datagram Transport Layer Security (DTLS)], чтобы обеспечить шифрование и конфиденциальность данных трафика мониторинга и управления. Другие безопасные протоколы, такие как HTTPS могут быть использованы для передачи трафика управления от сетевых устройств до сервера NMS или облачной платформы.
15. E. Большинство характеристик по безопасности находящиеся в контроллере БЛВС, также могут быть найдены в распределенной архитектуре БЛВС, даже несмотря то, что там нет контроллера БЛВС. Например, перехватывающий веб портал, который обычно находится в контроллере БЛВС, вместо этого находится в отдельных ТД (точках доступа). Межсетевой

**1010 Приложение А • Ответы на Контрольные Вопросы**

экран с учетом состояний соединений [stateful firewall] и функционал контроля доступа на основе ролей [role-based access control (RBAC)] находящиеся в центральном контроллере БЛВС, теперь присутствуют сообща [cooperatively] в ТД. Отдельная ТД может также работать как RADIUS сервер с возможностями интеграции с Легковесным Протоколом Доступа к Каталогу [Lightweight Directory Access Protocol (LDAP)]. Все механизмы плоскости контроля находятся в точках доступа на границе сети в распределенной архитектуре БЛВС.

16. D. Огромная масса устройств IoT с радиомодулем 802.11 на текущий момент передают только в полосе частот 2.4 ГГц. Пожалуйста, поймите, что не все устройства IoT используют Wi-Fi радиомодули. Устройства IoT могут использовать другие радиотехнологии такие, как Bluetooth или Zigbee. У устройств IoT также может быть Ethernet интерфейс в дополнение к радиоинтерфейсам.
17. A. За последнее десятилетие произошел взрывной рост парка клиентских ручных мобильных устройств, таких как смартфоны и планшеты. Большинство пользователей теперь ожидают получать подключение к Wi-Fi с многочисленных ручных мобильных устройств, а также с ноутбуков. Почти все мобильные устройства используют одночиповый форм фактор [single chip form factor], который встроен в материнскую плату устройства.
18. B. В централизованной архитектуре БЛВС, трафик туннелируется от ТД (точек доступа), управляемых только контроллером, установленных на уровне доступа, до контроллера БЛВС, который обычно развернут в ядре сети. Стандартный сетевой дизайн предполагает резервирование в ядре, и резервные контроллеры БЛВС должны быть установлены так, чтобы не было единой точки отказа сети. Если весь пользовательский трафик туннелирован до контроллера БЛВС, и он сломался без резервирования, то фактически БЛВС – легла.
19. A, B, C. Решения систем управления сетью [Network management system (NMS)] могут быть развернуты в Центре Обработки Данных компаний в форме аппаратного комплекса или виртуального комплекса, который работает на VMWare или какой-либо другой платформе виртуализации. Сервер системы управления сетью, который располагается в собственном центре обработки данных компании, часто называется, как on-premises NMS [NMS на своих площадях]. Решения NMS наиболее обычно доступны из облака, как сервис программного обеспечения по подписке [software subscription service].
20. B, D. Механизмы плоскости контроля работают в системе со взаимодействием между ТД с помощью протоколов совместной работы [cooperative protocols] в распределенной архитектуре БЛВС. В распределенной архитектуре, каждая индивидуальная точка доступа отвечает за локальную пересылку пользовательского трафика; следовательно, плоскость данных располагается в ТД. Плоскость управления располагается в системе управления сетью [network management system (NMS)], которая используется для управления и мониторинга распределенной БЛВС.

## Глава 12: Питание по Ethernet (PoE)

1. D. Даже когда 802.3af и 802.3at были поправками, PoE был определен с Статье 33 [Clause 33]. Когда поправки вошли в обновленный стандарт, нумерация статей сохранилась той же. Важно помнить номер статьи, поскольку обычно им оперируют при обсуждении PoE. Новая поправка 802.3bt определяет PoE по 4ем парам Ethernet в Статье 145 [Clause 145].**2.** А. Любое устройство, которое не предоставляет классификационную сигнатуру (которая является опциональной, т.е. не обязательной), автоматически считается устройством Класс 0, и PSE предоставит 15.4 ватта мощности этому устройству.

3. А, С. Стандарт Питание по Ethernet [Power over Ethernet (PoE)] определяет два типа устройств: питаемые устройства [powered devices (PDs)] и устройства подачи питания [power-sourcing equipment (PSE)].
4. Д. Питание, подаваемое к питаемому устройству [powered device (PD)], имеет номинал в 48 вольт; однако PD должно уметь принимать до 57 вольт.
5. А, В, С. Питаемое устройство [ powered device (PD)] должно быть способно принимать питание или по парам данных или по неиспользуемым парам, если это устройства 10BaseT или 100BaseTX , и по парам данных 1–2, 3–6 или парам данных 4–5, 7–8, если это устройство 1000BaseT. PD должно также отвечать оборудованию подачи питания [power-sourcing equipment (PSE)] классификационной сигнатурой. PD должно принимать питание с любой полярностью. Отвечать PSE классификационной сигнатурой является не обязательным.
6. Д. Предоставление классификационной сигнатуры является опциональным для питаемого устройства [powered device (PD)]. Если PD не предоставляет классификационную сигнатуру, устройство считается устройством Класса 0, и оборудование подачи питания [power-sourcing equipment (PSE)] будет выделять максимальную мощность. или 15.5 ватта.
7. С. До 802.3bt, PoE предоставлялся только по 2 парам Ethernet. С введением 802.3bt оборудование PSE, предоставляющее 45Вт, 60 Вт, 75Вт или 90 Вт использует 4 пары Ethernet и для конечного PSE и для промежуточного PSE.
8. Д. Устройства Класса 4 определены в поправке 802.3at. Максимальная мощность, которую требуют питаемые устройства [powered devices (PD)] Класса 4, между 12.95 и 25.5 ватт.
9. С. При максимальной мощности каждому устройству Power over Ethernet (PoE) будет предоставляться 30 ватт мощности от оборудования подачи питания [power-sourcing equipment (PSE)]. Если ко всем 24 портам подключены питаемые устройства (PD), то всего понадобится 720 ватт ( $30 \text{ ватт} \times 24 \text{ порта} = 720 \text{ ватт}$ ).
10. С. Оборудование подачи питания [power-sourcing equipment (PSE)] предоставляет девять потенциальных уровней мощности:
  - Класс 0 = 15.4 ватт
  - Класс 1 = 4.0 ватт
  - Класс 2 = 7 ватт
  - Класс 3 = 15.4 ватт
  - Класс 4 = 30.0 ватт
  - Класс 5 = 45 ватт
  - Класс 6 = 60 ватт
  - Класс 7 = 75 ватт
  - Класс 8 = 90 ватт

Так как это устройство требует 35 ватт мощности, от PSE будет требоваться предоставить 45 ватт.

11. Д. Оборудование подачи питания [power-sourcing equipment (PSE)] предоставляет питание в диапазоне от 44 вольт до 57 вольт, с номинальным питание в 48 вольт.
12. А. Максимальное расстояние в 100 метров является ограничением Ethernet, а нет ограничением Питания по Ethernet [Power over Ethernet (PoE)]. На 90 метрах это не

**1012 Приложение А • Ответы на Контрольные Вопросы**

проблема. Хотя конкретно в PoE стандарте не упоминается, кабели САТ 5е поддерживают связь 1000BaseT и, следовательно, способны также обеспечивать PoE. Большое количество PoE VoIP телефонов может потребовать больше мощности, чем коммутатор может предоставить, это приводит к тому, что точки доступа (ТД) начинают случайным образом перезагружаться [reboot].

- 13.** В. Коммутатор предоставит каждому устройству Класса 0 15.4 ватта мощности, а устройствам Класса 1 - 4 ватта мощности каждому. Поэтому 10 VoIP телефонов потребуют 40 ватт мощности, 10 точек доступа(ТД) потребуют 154 ватта мощности, и коммутатору нужно 500 ватт мощности - итого 694 ватта (40 Вт + 154 Вт + 500 Вт ).
- 14.** В. Коммутатор предоставит устройствам Класса 2 по 7 ватт мощности каждому, а устройствам Класса 3 по 15.4 ватта мощности каждому. Поэтому 10 камер потребуют 70 ватт мощности, 10 точек доступа (ТД) потребуют 154 ватта, а коммутатору нужно 1000 ватт - итого 1224 ватта (70 Вт + 154 Вт + 1000 Вт ).
- 15.** В, D. Применение Питания по Ethernet [Power over Ethernet (PoE)] не влияет на поддерживаемое расстояние Ethernet, которое является 100 метров или 328 футов.
- 16.** F. Питающие устройства (PD) 802.3bt потребляют до 71.3 ватта мощности.
- 17.** С. Максимальная мощность, используемая питающими устройствами (PD) Класса 0 - 12.95 ватт. Оборудование подачи питания [power- sourcing equipment (PSE)] подает 15.4 ватта из расчета сценария худшего случая, в котором могут быть потери мощности из-за кабеля и разъемов между PSE и PD. Максимальная мощность, используемая каждым классом:

Класс 1 PD = 3.84 ватт

Класс 2 PD = 6.49 ватт

Класс 3 PD = 12.95 ватт

Класс 4 PD = 25.5 ватт

Класс 5 PD = 40 ватт

Класс 6 PD = 51 ватт

Класс 7 PD = 62 ватт

Класс 8 PD = 71.3 ватт

- 18.** Е. Диапазон значений по разным классам:

Класс 0: 0–4 мА

Класс 1: 9–12 мА

Класс 2: 17–20 мА

Класс 3: 26–30 мА

Класс 4: 36–44 мА

- 19.** С. Альтернатива А использует 2 пары Ethernet для PoE, и принимает питание с обеими полярностями от источника питания по проводам 1, 2, 3, и 6. В альтернативе В, используются провода 4,5, 7, и 8.
- 20.** С. Устройства типов 2, 3, или 4 будут выполнять двух событийную классификацию Физического уровня или классификацию Канального уровня, которые позволят устройству

идентифицировать подключено оно к PSE Типу а или Типам 2, 3 или 4. Если взаимная идентификация не может быть завершена, то устройства могут работать как устройства Типа 1.

## Глава 13: Концепции Проектирования БЛВС

1. А. Если ТД и клиенты уже работают на DFS канале и обнаружен импульс от радара, то ТД и все ее ассоциированные клиенты должны уйти с канала. Если обнаружен радар на текущей DFS частоте, то ТД проинформирует все ассоциированные клиентские станции о перемещении на другой канал с помощью кадра оповещения о смене канала [channel switch announcement (CSA)]. У ТД и клиентов есть 10 секунд, чтобы уйти с DFS канала. ТД может послать несколько CSA кадров, чтобы гарантировать, что все клиенты ушли с канала. Кадр CSA уведомляет клиентов, что ТД переходит на новый канал, и что они должны перейти на этот канал тоже. В большинстве случаев, канал не-DFS и очень часто - это канал 36.
2. С. Балансировка нагрузки между точками доступа обычно применяется в тех местах, где очень высокая плотность клиентов и роуминг не является приоритетным — например, спортивный зал или аудитория с 20 ТД, установленных на одной и той же открытой территории. В этой среде клиент наиболее вероятно услышит все 20 ТД, и обычно требуется балансировка загрузки клиентов между ТД. Однако, в тех местах, где нужен роуминг, балансировка нагрузки не очень хорошая идея, потому что механизмы могут привести к тому, что клиенты станут залипшими и останутся ассоциированными с ТД слишком долго. Если кадры ответов на ассоциацию и переассоциацию от ТД задержатся, клиентская мобильность, вероятно, сломается. Балансировка нагрузки между ТД может быть губительной для процесса роуминга.
3. В, Д. Хотя полоса частот удвоена у 40 МГц каналов, из-за того, что существует мало доступных каналов, шанс ССI увеличивается. Точки доступа и клиенты на одном и том же канале могут слышать друг друга, а служебная информация [overhead] при борьбе за среду может негативно сказаться и убрать все достижения в производительности, которые дополнительная полоса может предоставить. Еще одна проблема с объединением каналов в том, что это приводит к уровню шума примерно на 3 дБ выше. Если уровень шума [noise floor] на 3 дБ, то SNR на 3 дБ ниже, что означает, что радиомодули фактически переключаются на более низкие скорости MCS, и, следовательно, более низкие модуляционные скорости передачи. Во многих случаях, это стирает некоторую часть улучшений, которые предоставляет 40 МГц частотное пространство.
4. Д. Многие профессионалы БЛВС советуют использовать 20 МГц каналы, а не 40 МГц каналы, в большинстве проектов 5 ГГц БЛВС. Однако, развертывание 40 МГц канала может работать при тщательном планировании и соблюдении нескольких общих правил.

Развертывание четырех или менее 40 МГц каналов в модели переиспользования будет недостаточно. Используйте 40 МГц каналы только, если доступны каналы DFS. Включение DFS каналов даст больше частотного пространства и, следовательно, больше доступных 40 МГц каналов для модели переиспользования. Не заставляйте радиомодули ТД передавать на полной мощности. Уровень мощности передачи в 12 дБм или ниже обычно более чем достаточен в большинстве сред внутри помещений. Стены должны быть из плотного материала в целях поглощения/затухания сигнала и уменьшения ССI. Шлакоблоки, кирпичи, или бетон приводят к затуханию сигнала на 10дБ и больше. Гипсокартон, однако, уменьшает сигнал только на 3дБ. Если установка происходит в многоэтажной среде, то рассмотрите отказ от использования 40 МГц каналов до тех пор, пока не будет достаточного затухания между этажами.

5. Е. Никто не любит этот ответ, но просто слишком много факторов, чтобы всегда давать один и тот же ответ для каждой ТД разных производителей БЛВС. Заводские настройки радиомодулей корпоративных БЛВС могут позволить 100–250 клиентский подключений. Так как большинство корпоративных ТД двух частотные, т.е. с радиомодулями 2.4ГГц и 5 ГГц, теоретически 200-500 клиентов может ассоциироваться с радиомодулями одной ТД. Хотя более 100 устройств может подключиться к радиомодулю ТД, это количество не реально для активных устройств из-за природы общедоступной полудуплексной среды. Потребности производительности этого множества клиентских устройств не будет удовлетворена, и пользовательский опыт будет плохого качества.
6. F. Три важных вопроса должны быть заданы относительно пользователей. Первый, скольким пользователям сейчас нужен беспроводной доступ, и сколько Wi-Fi устройств они будут использовать? Второй, скольким пользователям и устройствам может понадобиться беспроводной доступ в будущем? Эти первые два вопроса помогут вам начать адекватно планировать хорошее отношение устройств на точку доступа, учитывая при этом будущий рост. Третий вопрос огромного значения – где находятся пользователи и устройства? Также всегда помните, что все клиентские устройства не одинаковы. Многие клиентские устройства потребляют много эфирного времени из-за меньших или отсутствия функционала MIMO. В среднем 35-50 активных Wi-Fi устройств на радиомодуль, работающих через двухчастотную точку доступа 802.11 n/ac, является реалистичным при использовании приложений таких, как просмотр веб и работа с электронной почтой. Однако, приложения, интенсивно использующие полосу, такие как потоковое виде высокого качества, сильно скажется на производительность. Разные приложения требуют разное количество пропускной способности TCP.
7. A, D. Ответ действительно является делом вкуса и зависит от предпочтений профессионала БЛВС, также, как и тип проекта БЛВС. Возможности Адаптивного Радио [Adaptive RF] включены по умолчанию на большинстве ТД каждого производителя Wi-Fi. И алгоритмы RRM постоянно улучшаются год за годом. Основные заказчик коммерческого БЛВС используют RRM из-за простоты развертывания. RRM обычно является предпочтительным методом в установках на предприятиях с тысячами ТД. Однако, точные пояснения должны быть даны по использованию статического канала и настроек мощности в сложных радиосредах. Большинство производителей БЛВС рекомендуют в своих собственных руководствах по установке в очень плотных средах, чтобы использовались статическая мощности и каналы, особенно когда используются направленные антенны.
8. В. Исторически, самая большая проблема с использованием DFS каналов была в потенциальном ложно-положительном обнаружении радара. Другими словами, ТД ошибочно интерпретировала ложную радиопередачу за радар, и начинала изменение канала, даже если им не нужно было уходить с канала. Хорошая новость в том, что большинство

производителей корпоративных БЛВС стали лучше в уменьшении ложно-положительных обнаружениях. Использование каналов DFS всегда рекомендуется пока критически важные клиенты поддерживают их. Если поблизости действительно присутствует радар, просто уберите подверженные влиянию DFS каналы из 5ГГц частотного плана.

9. С. Е. Базовые скорости передачи данных, настроенные на ТД, считаются “требуемыми” скоростями для всех радиомодулей, работающих в BSS. ТД будет передавать все кадры управления и большинство кадров контроля на самой низкой настроенной базовой скорости. Кадры данных могут быть переданы с намного большей поддерживаемой скоростью передачи данных. Например, радиомодуль 5 ГГц ТД будет передавать все кадры маяки [beacon] и другой контрольный и управляющий трафик на 6 Мбит/с, если базовая скорость передачи радиомодуля настроена на ту скорость. Это потребляет огромное количество эфирного времени. Следовательно, распространенная практика – настраивать базовую скорость на 5 ГГц радиомодуле или на 12 Мб/с, или на 24Мб/с. Не настраивайте базовую скорость ТД на 18 Мб/с, потому что некоторые клиентские драйвера могут и не смочь интерпретировать ее.
10. С. Прежде чем ТД начнет передавать в первый раз на канале DFS, она должна произвести начальную проверку доступности канала [channel availability check (CAC)]. Радиомодуль ТД должен слушать в течении периода в 60 секунд прежде, чем можно будет передавать на канале. Если обнаружен какие-нибудь импульсы радара, то ТД не может использовать тот канал и должна попытаться использовать другой канал. Если никакого радара не обнаружено в течении начального 60 секундного периода прослушивания, то ТД может начать передачу кадров управления типа маяк [beacon] на канале. В Европе правила еще более строгие для каналов каналов 120, 124, и 128 Терминала Доплеровского Метеорологического Радара [Terminal Doppler Weather Radar (TDWR)]. ТД должна слушать 10 полных минут прежде чем можно передавать в TDWR пространстве частот.
11. Д. Одноканальная интерференция [Co-channel interference (CCI)] является самой основной причиной потребления эфирного времени [airtime] без необходимости, которое может быть минимизировано с помощью передового опыта надлежащего проектирования БЛВС. Клиенты являются причиной номер один CCI. Вам следует понимать, что CCI не статична, и всегда изменяется из-за мобильности клиентских устройств.
12. Е. Перекрытие зон не может быть измерено надлежащим способом. Перекрытие покрытий в действительности – это дублирование первичного и вторичного покрытия с точки зрения клиентской Wi-Fi станции. Надлежащее контрольное обследование [validation survey] должно быть проведено, чтобы гарантировать, что у клиента всегда есть адекватное задублированное покрытие от нескольких точек доступа. Другими словами, каждой клиентской Wi-Fi станции (STA) необходимо слышать, по крайней мере, одну точку доступа с определенным RSSI и резервную или вторичную точку доступа с другим RSSI. Обычно, большинство производителей требуют для порогов RSSI, чтобы приемный сигнал был -70 дБм для связи с высокоскоростной передачи данных. Следовательно, клиентской станции нужно слышать вторую ТД с сигналом в -75дБм или больше, когда сигнал, принятый от первой ТД, падает ниже -70 дБм.
13. Е. Чтобы уменьшить CCI, используйте на столько много каналов, насколько это возможно в 5 ГГц модели переиспользования каналов. Чем больше каналов используется, тем выше вероятность, что CCI может быть полностью уменьшена, включая одноканальную интерференцию, которая происходит от клиентских устройств. В большинстве случаев, вам следует использовать каналы динамического выбора частоты [dynamic frequency selection (DFS)] в 5 ГГц канальном плане.
14. Е. VoWiFi связь очень чувствительна к повторным передачам на 2ом уровне [layer 2

retransmissions]. Следовательно, когда вы проектируете БЛВС голосового уровня, то рекомендуется сигнал в  $-65$  дБм или сильнее так, чтобы принятый сигнал был значительно выше уровня шума. Рекомендуемое SNR для VoWiFi –  $25$ дБ. Принятый сигнал  $-70$  дБм и SNR  $20$  дБ обычно достаточно для высокоскоростного соединения для передачи данных.

15. D. Если ТД передает, все близко находящиеся точки доступа и клиенты на том же самом канале будут откладывать (задерживать) свои передачи. В результате пропускная способность неблагоприятно пострадает. Не нужная избыточная служебная информация [overhead] при борьбе за среду называется одноканальная интерференция [co-channel interference (CCI)]. В реалии, радиомодули 802.11 работают точно как определено CSMA/CA. CCI также иногда называется как перекрывающиеся базовые составы сервиса [overlapping basic service sets (OBSS)]. Хорошо спланированная модель переиспользования каналов может помочь минимизировать CCI в  $5$  ГГц полосе.
16. B. Перекрывающиеся зоны покрытия с перекрывающимися частотами вызывают интерференцию смежных каналов [adjacent channel interference], которая вызывает сильную деградацию в задержке, джиттере и пропускной способности. Если перекрывающиеся зоны покрытия также перекрываются по частотам, кадры будут становиться поврежденными, повторные передачи возрастут, и производительность значительно пострадает.
17. A. При проектировании беспроводной ЛВС вам понадобятся перекрывающиеся зоны покрытия для обеспечения роуминга. Однако, перекрывающиеся зоны не должны перекрываться по частотам. В Соединенных Штатах, только каналы  $1$ ,  $6$  и  $11$  следует использовать в полосе ISM  $2.4$  ГГц, чтобы получить наиболее доступные, неперекрывающиеся каналы. Перекрывающиеся зоны покрытия с перекрывающимися частотами вызывают, что называется интерференцию смежных каналов [adjacent channel interference]. Хотя четырехканальный план переиспользования можно использовать в Европе, трехканальная модель переиспользования все же остается рекомендованной.
18. B. Из-за мобильности и изменений в RSSI и SNR, клиентские станции и радиомодули ТД будут переключаться между скоростями передачи данных в процессе, который называется динамическое переключение скоростей [dynamic rate switching (DRS)]. Цель DRS в повышении или снижении скорости для оптимизации скорости и улучшения производительности. Хотя динамическое переключение скоростей является правильным наименованием для того процесса, все эти термины относятся к методу сброса скорости [speed fallback], который клиент беспроводного ЛВС и ТД используют по мере увеличения расстояния от точки доступа.
19. D. Мобильный клиент получает IP адрес, который также называется как домашний адрес, в исходной подсети. Мобильный клиент должен зарегистрировать свой домашний адрес на устройстве, которое называется домашний агент [home agent (HA)]. Исходная точка доступа в домашней сети клиента работает как домашний агент. HA – это единая точка контакта для клиента, когда он переходит через границы Зего уровня. Любой трафик, который посыпается на клиентский домашний адрес перехватывается точкой доступа-домашним агентом и посыпается через туннель Мобильного IP [Mobile IP] до ТД-внешнего агента [foreign agent AP] в новой подсети. Следовательно, клиент способен сохранить свой исходный IP адрес при роуминге через границы на Зем уровне.
20. C. Вероятностные формулы трафика используют телекоммуникационную единицу измерения, которая называется эрланг. Эрланг равен одному часу телефонного трафика за один час времени.

# Глава 14: Обследование места и Контрольное обследование

1. А, В, С. Хотя безопасность сама по себе не является частью обследования места БЛВС, тех, кто управляет сетью, стоит проинтервьюировать об ожиданиях о безопасности. Компании по обследованию дадут исчерпывающие рекомендации по беспроводной безопасности. Приложением к рекомендациям по безопасности могут быть рекомендации к корпоративной беспроводной политике. Решения по аутентификации [Authentication] и шифрованию [Encryption] обычно не применяются во время физического обследования.
2. А, В, Е. Любой тип радиоинтерференции может вызвать отказ в обслуживании [cause a denial of service] БЛВС. Обследование с анализом спектра следует выполнять, чтобы определить, вызывает ли больничное медицинское оборудование интерференцию в полосе ISM 2.4 ГГц или полосах U-NII 5 ГГц. Мертвые Зоны или потеря покрытия могут также прервать связь БЛВС. Многие больницы используют металлические сетчатые защитные стекла в некоторых местах. Металлическая сетка будет причиной рассеяния радиоволн и потенциальной потери покрытия с обратной стороны стекла. Лифтовые шахты сделаны из металла и часто являются мертвыми зонами, если покрыты радиосигналом ненадлежащим образом.
3. А, В, С, Д. Обследования вне помещений – это обычно обследования беспроводных мостов; однако, уличные точки доступа и взаимосвязные маршрутизаторы [mesh routers] также могут быть развернуты. Обследования вне помещений проводятся с помощью или уличных точек доступа или взаимосвязных маршрутизаторов [mesh routers], которые являются устройствами, обычно используемыми для предоставления доступа клиентским станциям в средах вне помещений. Эти уличные обследования Wi-Fi будут использовать большинство тех же самых инструментов, что и для обследования внутри помещений, но могут также использовать устройства глобально системы позиционирования [global positioning system (GPS)] для записи координат долготы и широты местоположения.
4. В. Хотя все варианты являются проблемами, которые нужно будет решать, при развертывании БЛВС в больничной среде, эстетика обычно является самым высшим приоритетом. Основные предприятия обслуживания клиентов предпочитают, чтобы все беспроводное оборудование оставалось полностью скрыто от взгляда. Заметьте, что большинство телекоммуникационных шкафов могут закрываться и помогают предотвратить кражу дорогостоящего оборудования Wi-Fi. Однако, предотвращение кражи не уникально для гостиниц.
5. А, С. Чертежи будут необходимы для интервью по обследованию места, чтобы обсудить потребности в покрытии и емкости. Карта сетевой топологии будет полезна при проектировании интеграции беспроводной сети в текущую проводную инфраструктуру.
6. Д. Хотя вариант С является возможным решением, лучшая рекомендация – то установка оборудования, которое работает в 5 ГГц. Большинство ТД уровня предприятия являются двухчастотными с радиомодулями 2.5 и 5 ГГц. Интерференция от сетей 2.4 ГГц соседних организаций никогда не будут проблемой с любым покрытием в 5 ГГц. 2.4 ГГц считается полос частот негарантированной доставки [best-effort frequency band]. Критическая Wi-Fi связь должна быть организована в 5 ГГц каналах.
7. А. Самое дешевое и наиболее эффективное решение было бы в замене старых пограничных коммутаторов на новые коммутаторы, у которых есть линейное питание, которое может предоставить PoE для точек доступа. Коммутатор ядра не используется для подачи PoE, из-за ограничений по длине кабеля. Установка однопортового инжектора не практично, и заказ работ электрика будет чрезвычайно дорогим.

8. Е. Несколько вопросов связано с интеграцией с инфраструктурой. Как точки доступа будут запитаны? Как БЛВС и/или пользователи БЛВС будут сегментированы (отделены) от проводной сети? Как будут управляться точки доступа удаленных БЛВС? Такие вопросы как управление доступом на основе ролей [role-based access control (RBAC)], управление полосой пропускания [bandwidth throttling], и балансировка нагрузки также следует обсудить.
9. А, В, С. Вам следует консультироваться с сетевыми администраторами [network management] во время большинства обследований и процесса установки, чтобы обеспечить надлежащую интеграцию БЛВС. Вам следует консультироваться с отделом технического обслуживания медицинской техники [biomedical department] относительно возможной радиоинтерференции. Вам следует связаться с охраной больницы [hospital security] для того, чтобы получить соответствующие пропуска и, возможно сопровождение.
10. А, В, Д. На основе информации, собранной во время обследования места, финальная схема проекта предоставляется заказчику. Вместе со схемами установки предоставляется детальная ведомость материалов [bill of materials (BOM)], которая перечисляет каждый компонент необходимого оборудования и программного обеспечения для финальной установки беспроводной сети. Следует подготовить предварительный детальный план-график установки, чтобы выделить все сроки, стоимость оборудования и стоимость работ.
11. Е. Во время активного ручного обследования радиокарта ассоциирована с точкой доступа и у нее есть связность на высоких уровнях, учитывающая низкоуровневую передачу кадров когда также производятся радиоизмерения. Главная цель активного обследования места – это посмотреть процент повторных передач на 2ом уровне.
12. А, С, Д. Измерительное колесо может быть использовано для измерения расстояния от коммутационной комнаты/шкафа до предполагаемого размещения точки доступа. Лестница или вилочный погрузчик могут быть нужны для временного монтажа точки доступа. Аккумуляторная батарея используется для питания точки доступа. GPS устройства используются вне помещений и не работают правильно внутри помещений. Микроволновые печи являются источниками интерференции.
13. В, Д. Беспроводные телефоны, которые работают в том же самом пространстве 5 ГГц U-NII полос могут вызвать интерференцию. Радар также является потенциальным источником интерференции в 5 ГГц. Микроволновые печи излучают в полосе ISM 2.4 ГГц. Радиомодули FM используют узкополосные передачи в низкочастотной лицензируемой полосе.
14. А, С. Во время пассивного ручного обследования радиокарта собирает радиоизмерения, включая силу принятого сигнала (дБм) [received signal strength (dBm)], уровень шума (дБм) [noise level (dBm)], и отношение сигнал-шум (дБ) [signal-to-noise ratio (dB)]. SNR – это мера разницы в децибелах (дБ) между принятым сигналом и фоновым шумом. Сила принятого сигнала – это абсолютное значение в дБм. Производители антенн определяют усиление с помощью или дБи, или дБд значений.
15. В, С, Д. Анализатор спектра следует использовать для сканирования полосы ISM 2.4 ГГц. Радиомодули Bluetooth, плазменные резаки [plasma cutters], и видео камеры 2.4 ГГц являются потенциальными интерферирующими устройствами.
16. А, Д. Где бы ни была размещена точка доступа во время обследования места, настройки мощности и канала должны быть записаны. Записывать настройки безопасности и IP адресов не необходимо.

17. С. Предиктивный анализ покрытия выполняется с помощью программного обеспечения, которое создает визуальные модели радиопокрытия и емкости, пропуская необходимость реального сбора радиопараметров. Проектируемые зоны покрытия создаются с помощью алгоритмов моделирования и значений затухания.
18. С. Сегментация, аутентификация, авторизация и шифрование следует обсудить во время интервью по обследованию места. Сегментация (разделение) трех типов пользователей на три отдельных VLANs с отдельными решениями по безопасности является самой лучшей рекомендацией. Пользователи данных, использующих 802.1X/EAP и CCMP/AES будут иметь самое сильное доступное решение. Так как у телефонов нет функции Корпоративный-Голос [Voice- Enterprise] или 802.11g, в качестве метода безопасности выбирается WPA-2. WPA-2 Personal обеспечивает голосовых пользователей шифрованием CCMP/AES также, но избегает использовать решение 802.1X/EAP, которое вызывает проблемы с задержкой. Как минимум, VLAN гостевых пользователей требует перехватывающий веб портал [captive web portal] и мощные гостевые политики межсетевого экрана.
19. D. Все профессионалы по обследованию соглашаются с важностью контрольного обследования [validation survey]. Подтверждение покрытия, производительность по емкости, и тестирование роуминга являются ключевыми компонентами надлежащего контрольного обследования. В зависимости от назначения беспроводной сети, могут быть использованы различные инструменты, чтобы помочь с контрольным обследованием места.
20. A, B, C, D. Обследования уличных беспроводных мостов требует множества вычислений, которые не нужны во время обследования внутри помещений. Вычисления бюджета линии связи, затухания при распространении в свободном пространстве [FPSL], чистота зоны Френеля, и запас на замирания являются необходимыми для любого канала связи типа мост.

## Глава 15: Решение проблем БЛВС

1. А. Независимо от сетевой технологии, основные проблемы случаются на Физическом уровне [Physical layer] модели OSI. Основные проблемы производительности и подключения в БЛВС 802.11 могут привести к Физическому уровню.
2. А, С, Е. Простое решение проблем с Wi-Fi [Wi-Fi Troubleshooting 101] гласит, что конечный пользователь сначала включает и выключает сетевую Wi-Fi карту. Это гарантирует, что драйвера сетевой карты (NIC) Wi-Fi взаимодействуют с операционной системой правильно. Пароль или парольная фраза, которая используется для создания PSK может быть 8-63 символов и всегда чувствительна к регистру. Проблема почти всегда в несовпадении учетных данных PSK. Если учетные данные PSK не совпадают, материализуется мастер парного ключа [pairwise master key (PMK)] не правильно создается и, следовательно, 4x-Стороннее Рукопожатие полностью проваливается. Еще одна возможная причина неудачи аутентификации PSK может быть несовпадение выбранного метода шифрования. Точка доступа может быть настроена, чтобы требовать только WPA2 (CCMP-AES), которую устаревшие WPA (TKIP) клиенты не поддерживают. Произойдет похожая ошибка 4x-Стороннего Рукопожатия.
3. С. Когда бы вы не решали проблемы с БЛВС, вам следует начать с Физического уровня, и 70 процентов случаев проблема будет находиться у клиента БЛВС. Если существует проблема с подключением клиента, Простое Решение Проблем БЛВС [WLAN Troubleshooting 101] гласит, чтобы вы выключили и заново включили сетевой БЛВС адаптер. Драйвер сетевой интерфейсной карты БЛВС является интерфейсом между радиомодулем 802.11 и операционной системой (OS) клиентского устройства. По какой-либо

**1020 Приложение A • Ответы на Контрольные Вопросы**

причине драйвер БЛВС и OS устройства могут не взаимодействовать корректно. Простое выключение/включение БЛВС NIC перезапустит драйвер. Проблемы клиентской безопасности обычно являются результатом неправильного ввода клиентских настроек.

4. A, B, C. Ошибка часто совершается, когда установленные точки доступа должны передавать на полной мощности. Фактически, это увеличивает зону действия точки доступа, но вызывает много проблем, которые обсуждались в той главе. Высокая мощность передачи для ТД внутри помещений обычно не будет удовлетворять потребностям в емкости. Увеличенные зоны покрытия могут вызвать проблемы скрытого узла. Точки доступа внутри помещений с полной мощностью станут причиной залипших клиентов и, следовательно, проблемами с роумингом. Точки доступа с полной мощностью вероятнее всего также увеличат шанс одноканальной интерференции [co-channel interference] из-за проникающих передач.
5. D. Если конечный пользователь жалуется на деградацию пропускной способности, возможна причина – скрытый узел. Анализатор протоколов -это полезный инструмент в определении проблемы скрытого узла. Если анализатор протоколов показывает высокую скорость повторных передач для MAC адреса одной станции при сравнении с другими клиентскими станциями, скорее всего скрытый узел найден. У некоторых анализаторов протоколов даже есть предупреждения [alarms] о скрытых узлах на основе порогов повторных передач.
6. C. В действительности все эти ответы правильные. Однако, если Эндрю спросил бы своего босса – почему он смотрит Facebook, Эндрю мог бы быть уволен. Варианты А и В являются технически корректными ответами, однако, его босс хочет только обвинить БЛВС. Помните, с точки зрения конечного пользователя, БЛВС всегда является виновником. Правильный вариант С, потому что босс Эндрю просто хочет исправить это.
7. B, D, E. Чрезмерные повторные передачи на 2ом уровне влияют на БЛВС двумя способами. Первый, повторные передачи уровня 2 увеличивают количество служебной информации MAC [MAC overhead] и, следовательно, уменьшают пропускную способность. Второе, если данные приложения должны быть повторно переданы на 2ом уровне, то время доставки трафика приложения задерживается и становится непоследовательным. Такие приложения как VoIP зависят от своевременной и последовательной доставки IP пакетов. Чрезмерные повторные передачи уровня 2 обычно приводят к увеличенной задержке и проблемам с джиттером для чувствительных ко времени приложений таких, как голос и видео.
8. D. Все эти ответы могут стать причиной неудачи 4x-Стороннего Рукопожатия между клиентом БЛВС и ТД в приемной. Драйверам Wi-Fi NIC нужно корректно взаимодействовать с операционной системой, чтобы PSK аутентификация была успешной. Если учетные данные PSK не совпадают, исходный материал парного мастер ключа [pairwise master key (PMK)] не корректно создается и, следовательно, 4x-Стороннее Рукопожатие полностью проваливается. Финальный Парный Временный Ключ [pairwise transient key (PTK)] никогда не создается. Помните, существует симбиотическая связь между аутентификацией и созданием динамических ключей шифрования. Если аутентификация PSK не проходит, то и 4x-Стороннее Рукопожатие, которое используется, чтобы создавать динамические ключи. Еще одна возможная причина неудачи аутентификации PSK может быть в несовпадении выбранного метода шифрования. Точка доступа может быть настроена требовать только WPA2 (CCMP-AES), которую устаревшие клиенты WPA (TKIP) не поддерживают. Может произойти похожая неудача с 4x-Сторонним Рукопожатием. Только вариант D верен, потому что проблема присутствует на одной ТД в приемной.
9. B, E, F. График показывает клиента [supplicant] и сервер RADIUS, пытающихся установить SSL/TLS туннель, чтобы защитить пользовательские учетные данные. SSL/TLS туннель

никогда не создастся и аутентификация будет не удачной. Это показатель того, что существует проблема с сертификатом. Весь диапазон проблем с сертификатами может быть причиной того, что SSL/TLS туннель не установится. Самые распространенные проблемы с сертификатом в том, что корневой сертификат ЦС [root CA certificate] устанавливается в некорректное хранилище сертификатов, выбран некорректный корневой сертификат, вышел срок серверного сертификата, закончился срок действия корневого сертификата ЦС [root CA certificate], или настройка времени у клиента некорректна.

10. А, D, E. Передовой опыт решения проблем гласит, что надлежащая информация будет собрана если задавать релевантные вопросы. Хотя варианты В и С могут быть интересны, они не релевантны к потенциальной проблеме.
11. B, D. VoWiFi требует, что бы переключение [handoff] было 150 мс или меньше, чтобы избежать деградации качества телефонного разговора, или еще хуже, потери соединения. Следовательно, требуется более быстрое, безопасное роуминговое переключение [faster, secure roaming handoffs]. Гибкое кэширование ключей [Opportunistic key caching (OKC)] и быстрый BSS переход [fast BSS transition (FT)] осуществляют переключение [handoffs] почти за 50 мс, даже когда 802.1X/EAP выбрано в качестве решения по безопасности. ТД и клиент должны поддерживать FT; иначе, клиент будет переаутентифицироваться каждый раз, когда клиент переключается.
12. A, B. Роуминговые проблемы происходят, если не достаточно дублированного вторичного покрытия. Отсутствие вторичного покрытия фактически создает роуминговую мертвую зону, и соединение может быть даже временно потеряно. С другой стороны, слишком много вторичных покрытий также вызовут роуминговые проблемы. Например, клиентская станция может оставаться ассоциированной с ТД и не подключиться ко второй точке доступа, даже если станция будет прямо под второй точкой доступа. Обычно это называется проблемой залипшего клиента.
13. A. Максимальная длина в 100 метров – это ограничение Ethernet, а не ограничения PoE. На 90 метрах это не проблема. Хотя конкретно не упоминается в стандарте PoE, кабели Категории 5e поддерживают связь 1000BaseT, а следовательно, способны также обеспечить PoE. Питание, требуемое большим количеством настольных VoIP телефонов с PoE может превысить бюджет мощности PoE коммутатора. В большинстве случаев, основная причина случайной перезагрузки ТД в том, что бюджет мощности коммутатора был исчерпан.
14. C. Команда **netsh** (network shell) может быть использована для настройки и решения проблем и с проводным и беспроводным сетевыми адаптерами в компьютере с Windows. Команды **netsh wlan show** представляют детальную информацию относительно Wi-Fi радиомодуля, используемого компьютером с Windows. Сравнимая утилита командной строки для настройки и решения проблем сетевых адаптеров 802.11 в macOS компьютерах – это **airport**. При подготовке к экзамену CWNA, уделите время познакомиться с командами **netsh wlan** для Windows. Знакомство с командами **airport** для macOS может быть также полезным. AsKak с любой командой CLI, наберите команду **?**, чтобы посмотреть все варианты.
15. A, B, C. Передовой опыт решения проблем гласит, что надлежащая информация будет собрана, если задавать релевантные вопросы. Вариант D – это вопрос, заданный хранителем моста в знаменитом фильме Монти Пайтон [Monty Python].
16. C, D. Хотя все эти ответы могут быть причиной неудачи IPsec VPN, только две из них проблемы связаны с проблемой с сертификатами во время IKE Фазы 1. Если IKE Фаза 1 не проходит из-за проблемы с сертификатом, убедитесь, что у вас корректные сертификаты установлены корректно на конечных точках VPN. Также помните, что сертификаты основаны на времени. Очень часто проблема с сертификатами во время IKE Фазы 1 – это просто некорректная настройка часов на любом из концов VPN. Если настройки хеша и шифрования не совпадают на обоих сторонах, VPN не установится во время IKE Фаза 2. Если настройки публичного/приватного IP адреса ошибочны, VPN не установится во время IKE

17. А, F. График ясно показывает, что аутентификация 802.1X/EAP полностью выполнена и 4x-Стороннее Рукожатие создает динамические ключи шифрования для ТД и клиентского радиомодуля. В этой точке, аутентификация на 2ом уровне выполнена и виртуальный контролируемый порт на точке доступа открыт для клиента. Однако, клиенту не удается получить IP адрес. Это не проблема 802.1X/EAP, а сетевая проблема. Не корректная настройка пользовательского VLANa на коммутаторе могла вызвать ту проблему. Еще одна потенциальная причина могла быть в том, что DHCP выключен или закончились адреса для раздачи.
18. F. Проблема скрытого узла встает, когда клиентские станции не могут слышать радиопередачи другой клиентской станции. Увеличивая мощность передачи клиентской станции увеличит дальность передачи каждой станции, приводя к увеличению вероятности того, что все станции услышат друг друга. Однако, увеличение клиентской мощности не является рекомендованным решением, потому что передовой опыт гласит, что клиентские станции используют одну и ту же мощность передачи, используемую всеми другими радиомодулями в BSS, включая ТД. Уменьшение клиентской мощности также может привести к большему количеству скрытых узлов. Перемещение скрытого узла в зону действия передачи других станций также приведет к тому что станции будут слышать друг друга. Устранение препятствия, которое препятствовало тому чтобы станции слышали друг друга, также исправит ту проблему. Однако, лучшее решение повторяющейся проблемы скрытого узла – это добавить еще одну точку доступа в области, где находится скрытый узел.
19. B, D, E. Если какая-либо часть одноканального [unicast] кадра повреждена, циклическая избыточная проверка [cyclic redundancy check (CRC)] не пройдет, и приемный радиомодуль 802.11 не вернет кадр ACK передающему радиомодулю 802.11. Если кадр ACK не получен исходным передающим радиомодулем, то одноканальный [unicast] кадр не подтвержден, и должен быть отправлен повторно. Радиointерференция, низкое SNR, скрытые узлы, несовпадающие настройки мощности, и интерференция смежных каналов могут вызвать повторные передачи на 2ом уровне. Одноканальная интерференция на вызывает повторных передач, но добавляет ненужную служебную информацию [overhead] при борьбе за среду.
20. D. Если существует какая-либо клиентская проблема с подключением, Простое решение проблем гласит, что вы должны выключить и заново включить сетевой БЛВС адаптер. Драйвера сетевой интерфейсной карты (NIC) БЛВС являются интерфейсом между радиомодулем 802.11 и операционной системой (OS) клиентского устройства. По разным причинам, драйвера БЛВС и OS устройства могут не взаимодействовать корректно. А простое выключение/включение БЛВС NIC перезапустит драйверы. Всегда убирайте ту потенциальную проблему, прежде чем исследовать что-либо еще.

## Глава 16: Беспроводные Атаки, Мониторинг Вторжения, и Политика

1. В, С. Атаки отказа в обслуживании [Denial-of-service (DoS)] могут происходить как на 1ом уровне, так и на 2ом уровне модели OSI. Атаки на 1ом уровне называются атаками постановки радиопомех [RF jamming attacks]. Широкое разнообразие DoS атак на 2ом уровне является результатом манипуляции с кадрами 802.11, включая подмену кадров деаутентификации [spoofing of deauthentication frames].
2. С, D. Злонамеренное подслушивание [Malicious eavesdropping] получается неавторизованным использованием анализатора протоколов для перехвата беспроводной связи. Любая незашифрованная передача кадров 802.11 может быть восстановлена на

3. D. Анализатор протоколов – это пассивное устройство, которое перехватывает(записывает) трафик 802.11 и, которое может быть использовано для злонамеренного подслушивания. Система предотвращения беспроводных вторжений [wireless intrusion prevention system (WIPS)] не может обнаружить пассивное устройство. Сильное шифрование является решением для предотвращения атак злонамеренного подслушивания .
4. C, D. Единственный способ предотвратить беспроводной угон [wireless hijacking], человек-по-середине [man-in-the-middle], и фишинговый Wi-Fi атаки – это использование решения взаимной аутентификации. Решения по аутентификации 802.1X/EAP требуют, чтобы сначала происходил обмен взаимными аутентификационными учетными данными [mutual authentication credentials] прежде, чем пользователь мог быть авторизован.
5. F. Даже с лучшей аутентификацией и шифрованием, атакующие все еще могут видеть информацию о MAC адресе открытым текстом. MAC адреса нужны для направления трафика на 2ом уровне, и никогда не шифруются. Можно установить ограничения на устройства с помощью фильтрации по MAC [MAC filtering]. Однако, MAC фильтры можно легко обмануть с помощью подмены MAC [MAC spoofing].
6. A, B. Общая политика беспроводной безопасности определяет почему политика беспроводной безопасности нужна для организации. Даже если у компании нет планов по развертыванию беспроводной сети, должна быть, как минимум, политика уточняющая как поступать с неучтенными [rogue] беспроводными устройствами. Рабочая политика безопасности [functional security policy] определяет как обезопасить беспроводную сеть в терминах того, какие решения и какие действия нужны.
7. A, E. После получения парольной фразы [passphrase], атакующий может ассоциироваться с точкой доступа WPA/WPA2, и таким образом получить доступ к сетевым ресурсам. Технология шифрования не взломана, но ключ может быть воссоздан. Если у хакеров есть парольная фраза [passphrase] и перехват 4x-Стороннего Рукопожатия [4-Way Handshake], они могут воссоздать динамические ключи шифрования и, следовательно, расшифровать трафик. WPA/WPA2- Personal не считаются сильными безопасными решениями для предприятий, потому что, если парольная фраза скомпрометирована, атакующий может получить доступ к сетевым ресурсам и расшифровать трафик.
8. A, C, D, E. Существуют многочисленные типы атак отказа в обслуживании (DoS) на 2ом уровне, включая потоки на ассоциацию [association floods], подделка деаутентификации [deauthentication spoofing], подделка деассоциации [disassociation spoofing], поток на аутентификацию [authentication floods], поток запросов PS-Poll [PS-Poll floods], и атаки на виртуальную несущую. Постановка радиопомех [RF jamming] – это атака DoS на 1ом уровне. Механизмы защиты кадров управления 802.11w (MFP) могут уменьшить некоторые из большинства DoS аттак на 2ом уровне, но не все из них.
9. A, C. Микроволновые печи работают в полосе ISM 2.4 ГГц и часто являются источником непреднамеренной интерференции. Беспроводные телефоны в 2.4 ГГц также могут вызвать непреднамеренные помехи. Генератор сигналов обычно предполагается использовать как устройство постановки помех [jamming device], которые могут считаться преднамеренными помехами. Беспроводной телефон в 90 МГц не интерферирует с оборудованием 802.11, которое работает в полосе ISM 2.4 ГГц или полосах U-NII 5 ГГц. Не существует такой вещи как деаутентификационный передатчик [deauthentication transmitter].
10. C, D, E. Большинство неавторизованных устройств (или устройств без разрешения) [unauthorized devices], размещенных в сети, называются как неучтенные [rogues], и устанавливаются людьми с доступом к зданию. Это означает, что они более часто устанавливаются людьми, которым вы доверяете: сотрудники, подрядчики, и посетители.

**1024      Приложение А • Ответы на Контрольные Вопросы**

Вардрайверам [Wardrivers] и атакующим обычно физически доступ не разрешен.

11. A, C. Изоляция клиентов [Client isolation] – это функция, которая может быть включена на точке доступа БЛВС или контроллере БЛВС, чтобы заблокировать беспроводных клиентов от взаимодействия с другими беспроводными клиентами на одном и том же VLANe и IP подсети. Персональный межсетевой экран [personal firewall] может также использоваться для уменьшения атак равный-с-равным [peer-to-peer attacks].
12. C. Система предотвращения беспроводного вторжения [wireless intrusion prevention system (WIPS)] способна уменьшить атаки от неучтенных [rogue] точек доступа (NL). Сенсор WIPS может использовать атаки 2ого уровня в качестве контрмеры против неучтенного устройства [rogue device]. Можно также использовать выключение порта [Port suppression], чтобы выключить порт коммутатора, в который включена неучтеннная [rogue] ТД. Производители WIPS также используют непубликуемые методы для уменьшения атак от неучтенных устройств [rogue attacks].
13. A, B, E, F. Большинство решений WIPS маркирует радиомодули 802.11 на четыре (иногда на больше чем четыре) классификации. Авторизованное устройство относится ко всем клиентским станциям или ТД, которые являются авторизованными членами беспроводной сети компании. Неавторизованное/неизвестное устройство – это любой новый радиомодуль 802.11, который был обнаружен, но не классифицирован как неучтенный [rogue]. Соседнее устройство относится к любой клиентской станции или ТД, которое обнаружено WIPS и идентифицировано как интерферирующее устройство, но не обязательно считается угрозой. Неучченное устройство [rogue device] относится к любой клиентской станции или ТД, которое считается интерферирующими устройство и потенциальной угрозой.
14. A, E. Каждой компании следует иметь политику запрещающую установку беспроводных устройств сотрудниками. Каждой компании также следует иметь политику по тому как реагировать на все беспроводные атаки, включая обнаружение неучтенных [rogue] ТД. Если WIPS обнаружила неучченную [rogue] ТД, то советуются временное применение средств сдерживания неучтенных [rogue] устройств на 2ом уровне до тех пор, пока не будет обнаружено физическое местоположение неучтенного [rogue] устройства. После того, как устройства найдено, немедленно отключите его порта данных, но не из электрической розетки. Советуется оставить неучченную [rogue] ТД так, чтобы администратор мог сделать некоторые расследования и посмотреть на таблицы ассоциаций и лог файлы, для возможного определения кто установил ее.
15. A, C, D, F, G. На текущий момент, нет такой вещи как атака Счастливой ТД [Happy AP attack] или атак небесных обезьян 802.11 [802.11 sky monkey attack]. Беспроводные пользователи особенно уязвимы к атакам в публичных хотспотах, потому что там нет безопасности. Так как не используется никакого шифрования, беспроводные пользователи уязвимы для злонамеренного подслушивания. Так как нет взаимной аутентификации, они уязвимы к угону [hijacking], человек-по-середине [man-in-the-middle], и фишинговым атакам. ТД хотспота также может разрешать связь равный-с-равным, делая пользователей уязвимыми к атакам равный-с-равным [peer-to-peer attacks]. Каждой компании следует иметь политику безопасности по удаленному беспроводному доступу, чтобы защитить своих конечных пользователей, когда они покидают территорию компании.
16. A, C. Хотспоты с публичным доступом абсолютно не имеют безопасности, потому в приказном порядке необходимо, чтобы политика удаленного доступа к БЛВС строго соблюдалась. Эта политика должна включать требуемое к использованию решение IPsec или SSL VPN, чтобы обеспечить аутентификацию устройства, аутентификацию пользователя, и сильное шифрование всего беспроводного трафика данных. Хотспоты являются первичной целью для атак злонамеренного подслушивания. Персональные межсетевые краны должны быть установлены на всех удаленных компьютерах, чтобы предотвратить атаки равный-с-равным [peer-to-peer]

17. В. MAC фильтры настраиваются, чтобы применить ограничения, которые позволяют пройти только трафику от определенных клиентских станций на основе их уникальных MAC адресов. MAC адреса могут быть подменены, или подделаны, и любой хакер-любитель может легко пройти любой MAC фильтр подменой на разрешенный адрес клиентской станции.
18. А. Интегрированные системы предотвращения беспроводных вторжений [wireless intrusion prevention system (WIPS)] намного более широко установлены. WIPS, устанавливаемые поверх, обычно недоступные по цене для большинства заказчиков БЛВС. Более надежные устанавливаемые поверх решения WIPS обычно устанавливаются в оборонных, финансовых и розничных вертикальных рынках, где бюджет для выделенных решений может быть доступен.
19. А, Д. Шифрование эквивалента проводной конфиденциальности [Wired Equivalent Privacy (WEP)] было взломано, и на текущий момент доступные инструменты могут легко вычислить секретный ключ за минуты. Размер ключа не имеет значения; и 64-битный WEP и 128-битный WEP были взломаны. Шифрование CCMP/AES и 3DES не было взломано.
20. Д. Атака, которая часто создает много шумихи в прессе – это беспроводной угон [wireless hijacking], также называется как атака злого двойника [evil twin attack]. Атакующий уводит клиентов на уровне 2 и уровне 3 с помощью точки доступа – двойника [evil twin access point] и DHCP сервера. Хакер может провести атаку в несколько шагов, и запустить атаку человек-по-середине [man-in-the-middle] и/или фишинговую Wi-Fi атаку.

## Глава 17: Архитектура Сетевой Безопасности 802.11

1. D, F. WPA2-Enterprise и WPA3-Enterprise используют безопасность 802.1X/EAP. Как требуется решением безопасности 802.1X, клиент – это клиент БЛВС, требующий аутентификации и доступ к сетевым ресурсам. Каждое приложение имеет уникальные учетные данные аутентификации, которые подтверждаются сервером аутентификации.
2. E. 192 битный режим WPA3-Enterprise может быть развернут в чувствительных корпоративных средах для дальнейшей защиты Wi-Fi сетей с более высокими требованиями к безопасности, такие как правительственные учреждения, оборонные, и промышленные. Это опциональный режим, использующий минимальную силу в 1932 бита протокол безопасности и криптографические инструменты, чтобы лучше защитить чувствительные данные. 256-битный GCMP/AES используется для шифрования кадров данных вместо стандартного CCMP/AES со 128битным шифрованием. 256-битный Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP- GMAC-256) также требуется для защиты кадров управления.
3. E. 128-битное WEP шифрование использует секретный 104-битный статический ключ, который предоставляется пользователем (26 шестнадцатеричных символа) и комбинируются с 24 битным вектором инициализации [24-bit initialization vector (IV)] для фактической силы ключа в 128 битов.
4. А, С, Е. Структура авторизации 802.1X состоит из трех главных компонентов, каждый с

определенной ролью. Компоненты работают вместе, чтобы гарантировать, что только надлежащим образом подтвержденные пользователи и устройства авторизованы для доступа к сетевым ресурсам. Клиент запрашивает доступ к сетевым ресурсам; сервер аутентификации аутентифицируют личность клиента; и аутентификатор разрешает или запрещает доступ к сетевым ресурсам через виртуальные порты. Протокол аутентификации уровня 2, называемый Расширяемый Протокол Аутентификации [Extensible Authentication Protocol (EAP)] используется в структуре 802.1X для подтверждения пользователей на уровне 2.

5. С Сертификация WPA3-Personal Wi-Fi Альянса определяет одновременную аутентификацию равных [simultaneous authentication of equals (SAE)] как более надежную замену для аутентификации с заранее известным общим ключом [preshared key (PSK)]. WPA3- Personal (SAE) заменяет WPA2-Personal (PSK). Основная цель SAE в предотвращении усиленных атак перебора по словарю [brute-force dictionary attacks], к которым учетные данные PSK чувствительны.
6. D. Самая большая проблема с использованием аутентификации PSK на предприятиях – это социальная инженерия. PSK один и тот же на всех устройствах БЛВС. Если конечный пользователь случайно выдаст PSK хакеру, то безопасность БЛВС скомпрометирована. Если сотрудник покидает компанию, все устройства должны быть перенастроены на новый 64-битный PSK, что создает много работы администратору. Несколько производителей БЛВС предлагают проприетарные решения PSK, в которых у каждого индивидуального устройства будет свой собственный уникальный PSK. Решение PSK на устройство, на пользователя устраниет бремя администратора по перенастройке каждого БЛВС устройства конечного пользователя.
7. A, B, D. WEP, TKIP, и CCMP используют симметричные шифры. WEP и TKIP используют шифр ARC4, и CCMP используют шифр AES. Криптография публичного ключа [Public-key cryptography] основана на асимметричной связи.
8. A, B. Миграция с TKIP на CCMP может быть видна в стандарте IEEE 802.11-2020, который гласит, что скорости передачи данных схемы кодирования и модуляции 802.11n/ac не разрешены к использованию, если включены WEP или TKIP. Это исключение было решено в 2012 году и IEEE и Wi-Fi Альянсом. Дополнительно, TKIP не может быть использован для скоростей передачи данных 802.11ax. CCMP это назначенный метод шифрования для скоростей передачи данных 802.11n/ac/ax. Поправка 802.11ad-2012 стандартизовала использование Протокола Режима Счетчика/Галуа [Galois/Counter Mode Protocol (GCMP)], который использует AES криптографию. Чрезвычайно высоким скоростям передачи, определенным в 802.11ad, нужен GCMP, потому что он более эффективен, чем CCMP. GCMP также считается optionalным методом шифрования.
9. A, B, C, D, E. Три главные компоненты подхода RBAC – это пользователи, роли и разрешения. Отдельные роли могут быть созданы, такие как роль продавцов или роль маркетинга. Разрешения пользовательского трафика могут быть определены как разрешения на 2ом уровне (MAC фильтры), VLANы, разрешения на 3ем уровне (списки контроля доступа [access control lists]), разрешения уровней 4–7 (правила межсетевого экрана с учетом состояний), и разрешения по ширине полосы. Все эти разрешения могут также быть на основе времени. Разрешения пользовательского трафика ставятся в соответствие с ролями. Некоторые производители БЛВС используют термин “роли”, когда другие производители используют термин “пользовательские профили”.
10. D. VPNы наиболее часто используются для безопасности на основе клиента при подключении к БЛВС с публичным доступом и хотспотам, которые не предоставляют безопасность. Так как большинство хотспотов не обеспечивают Wi-Fi безопасность, обязательно, чтобы конечные пользователи обеспечивали свою собственную безопасность. Еще одно общее использование технологии VPN – предоставление соединения точка-точка [site-to-site] между удаленным

офисом и корпоративным офисом через распределенный WAN канал. Когда установлены мосты БЛВС для беспроводной транзитной связи, технология VPN может быть использована для обеспечения необходимого уровня конфиденциальности данных.

11. В. Инкапсулированное внутрь тела кадра кадра данных 802.11 является полезной нагрузкой верхних уровней, которая называется блоком данных MAC сервиса [MAC service data unit (MSDU)]. MSDU содержит данные от Контроля Логического Канала Связи [Logical Link Control (LLC)] и уровней 3–7. MSDU – это полезная нагрузка данных, которая содержит IP пакет плюс некоторые данные LLC. Когда включено шифрование, полезная нагрузка MSDU внутри кадра данных 802.11 зашифрована.
12. В, D, E. Аутентификация с общим ключом [Shared Key authentication] является устаревшим методом аутентификации, который не предоставляет исходный материал для генерации динамических ключей шифрования. Статический WEP использует статические ключи. Ассоциация надежной безопасной сети [robust security network] требует четырех-кадровый обмен EAP, который называется как 4x-Стороннее Рукожатие, которое используется для генерации динамических CCMP ключей. Рукожатие может происходить или после обмена 802.1X/EAP, или как результат аутентификации PSK или SAE.
13. А, D. Решение 802.1X/EAP требует, чтобы и клиент и сервер аутентификации поддерживали один и тот же тип EAP. Аутентификатор должен быть настроен на аутентификацию 802.1X/EAP, а не заботиться какой тип EAP пропускать. Аутентификатор и клиент должны поддерживать один и тот же тип шифрования.
14. С. Контроллер БЛВС обычно централизуют плоскость данных, и весь трафик EAP туннелируется между ТД и контроллером БЛВС. Контроллер БЛВС является аутентификатором. Когда развернуто решение 802.1X/EAP в среде с беспроводным контроллером, то на контроллере БЛВС присутствуют виртуальный контролируемый и неконтролируемый порты.
15. Е. Несколько примеров использования учетных данных PSK на-пользователя и на-устройство получили популярность на предприятиях. Однако, проприетарное применение аутентификации PSK не означает замену для 802.1X/EAP.
16. А, D, E. Назначение аутентификации 802.1X/EAP – аутентификация пользовательских учетных данных и авторизация (разрешение) доступа к сетевым ресурсам. Хотя структура 802.1X не требует шифрования, настойчиво рекомендуется использовать шифрование. Побочный продукт 802.1X/EAP – генерация и распространение динамических ключей шифрования. Хотя процесс шифрования действительно является побочным продуктом процесса аутентификации, цели аутентификации и шифрования совершенно различны. Аутентификация предоставляет механизмы для подтверждения личности пользователя, в то время как шифрование предоставляет механизмы конфиденциальности данных.
17. Д. Алгоритм AES шифрует данные в фиксированные блоки данных с выбором силы ключа шифрования в 128, 192, или 256 бит. CCMP/AES использует 128-битный ключ шифрования и шифрует в 128-битные фиксированной длины блоки.
18. А, D, F. Сертификация WPA2 требует использование метода аутентификации 802.1X/EAP на предприятии и использование аутентификации PSK в среде SOHO. Сертификация WPA2 также требует использование более сильных методов генерации динамических ключей шифрования. Шифрование CCMP/AES является обязательным методом шифрования, а TKIP/ARC4 является опциональным методом шифрования. Аутентификация SAE определена для WPA3. Динамическое WEP шифрование никогда не было определено Wi-Fi Альянсом для безопасности.
19. В, С, Е. 192-битный режим WPA3-Enterprise означает, что будет развернут в

чувствительных корпоративных средах для большей защиты Wi-Fi сети с более высокими требованиями по безопасности, например правительственные учреждения, оборонные и промышленные предприятия. 256-битный GCMP/AES используется для шифрования кадров данных вместо стандартного CCMP/AES с 128 битным шифрованием. BIP-GMAC-256 для защиты кадров управления используется вместо обычного согласуемого BIP-CMAC-128. Требуется использовать EAP-TLS в качестве протокола аутентификации.

20. С. Клиент, аутентификатор, и сервер аутентификации работают вместе для обеспечения структуры контроля доступа на основе порта 802.1X, и протокол аутентификации нужен для помощи в процессе аутентификации. Расширяемый Протокол Аутентификации [Extensible Authentication Protocol (EAP)] используется для обеспечения аутентификации пользователя или устройства.

## Глава 18: Приноси Свое Собственное Устройство (BYOD) и Гостевой Доступ

1. В, С, Е. Порты межсетевого экрана, которые должны быть разрешены включают UDP порт 67 DHCP сервера, UDP порт 53 DNS, TCP порт 80 для HTTP, и TCP порт 443 для HTTPS. Это позволит гостевым пользовательским беспроводным устройствам получить IP адрес, выполнить запрос к Системе Доменных Имен [Domain Name System (DNS)], и просматривать веб. Многие компании требуют, чтобы их сотрудники использовали подключения безопасной виртуальной частной сети [virtual private network (VPN)], когда они подключены к идентификатору сервисного состава [service set identifier (SSID)] отличному от SSID компании. Следовательно, рекомендуется, чтобы UDP порт 500 IPsec IKE и UDP порт 4500 IPsec NAT-T также были разрешены.
2. А, Е. Гостевая политика межсетевого крана должна разрешать Протокол Динамической Конфигурации Хостов [Dynamic Host Configuration Protocol (DHCP)] и Систему Доменных Имен [Domain Name System (DNS)], но ограничивать доступ к частным сетям 10.0.0.0/8, 172.16.0.0/12, и 192.168.0.0/16. Гостевые пользователи не разрешены в этих частных сетях, так как корпоративные сетевые сервера и ресурсы обычно находятся в частном IP пространстве. Гостевая политика межсетевого крана должна просто маршрутизировать весь гостевой трафик прямо на шлюз в Интернет и прочь от корпоративной сетевой инфраструктуры.
3. А, Д, Е. Четыре главных компонента архитектуры упраждления мобильными устройствами [mobile device management (MDM)] – это мобильное устройство, точка доступа (ТД) и/или контроллер БЛВС, сервер MDM, и сервис push уведомлений. Мобильное Wi-Fi устройство требует доступ к корпоративной БЛВС.

ТД или контроллер БЛВС помещают в карантин мобильное устройство внутрь огороженного сада [walled garden], если устройства не были зарегистрированы через MDM сервер. MDM сервер отвечает за регистрацию клиентских устройств. Сервисы Push уведомлений, такие как сервис Push Уведомлений Apple [Apple Push Notification service (APNs)] и Облачные Сообщения Google [Google Cloud Messaging (GCM)], взаимодействующие с мобильными устройствами и MDM серверами через управление-через-эфир [over-the-air management].

4. А, С. 802.1X/EAP требует, чтобы корневой сертификат ЦС [root CA certificate] был установлен на клиенте. Установка корневого сертификата на ноутбуки Windows могут быть легко автоматизированы с помощью Объектов Групповых Политик [Group Policy Object (GPO)]. Управление мобильными устройствами [Mobile device management (MDM)]

использует оснащение через эфир [over-the-air provisioning] для мобильных устройств прошедших регистрацию, и размещает корневой сертификат ЦС на мобильных устройствах, которые используют безопасность 802.1X/EAP. Приложения по самостоятельной регистрации устройств могут также быть использованы для передачи корневых сертификатов ЦС на мобильные устройства. Техническая спецификация Хотспот 2.0 также определяет методы автоматического оснащения сертификатами для идентификаторов сервисных составов (SSID) Пасспоинта.

5. Д. Клиентские устройства сертифицированные для Пасспоинт опрашивают БЛВС до подключения для того, чтобы обнаружить сотовых сервис провайдеров, поддерживаемых сетью. Устройства используют Протокол Опроса Сетей Доступа [Access Network Query Protocol (ANQP)], протокол запросов и ответов, определенный 802.11u. Другая информация, такая как поддерживающие методы EAP и роуминговые соглашения с сервис провайдерами, также могут быть предоставлены через запросы ANQP.
6. В, D, E. Сервер управления мобильными устройствами [mobile device management (MDM)] может мониторить информацию мобильного устройства, включая наименование устройства, серийный номер, емкость, срок жизни батареи, и приложения, которые установлены на устройстве. Информация, которую нельзя видеть, включает сообщения сервиса коротких сообщений [short message service (SMS)], персональную электронную почту, календари, и историю браузера.
7. В, D. Как определено спецификацией Хотспот 2.0, четыре метода Расширяемого Протокола Аутентификации [Extensible Authentication Protocol (EAP)], которые могут быть использованы для аутентификации клиентом Пасспоинта – это EAP-SIM, EAP-AKA, EAP-TLS, и EAP-TTLS. Современные 3G/4G сотовые смартфоны используют EAP-AKA с учетными данными SIM карты. EAP-TLS или EAP-TTLS может быть использован для не-SIM клиентов, таких как ноутбуки.
8. А, В, Е. Решение перехватывающего портала [captive portal] фактически включает веб браузер в сервис аутентификации. Чтобы аутентифицироваться, пользователь должен запустить веб браузер. После того как браузер запущен и пользователь попытался зайти на веб сайт, не важно какую вею страницу пользователь попытался открыть, пользователь перенаправляется на приглашение ввода логина [login], которое является веб страницей ввода логина перехватывающего портала [captive portal]. Перехватывающие порталы могут перенаправлять неаутентифицированных пользователей на страницу логина [login] с помощью перенаправления по IP [IP redirection], перенаправления по DNS [DNS redirection], или перенаправления HTTP [HTTP redirection].
9. В, С, D. Точка доступа (ТД) держит мобильные клиентские устройства внутри огороженного сада [walled garden]. В развернутой сети огороженный сад [walled garden] – это закрытая среда, которая ограничивает доступ к веб содержимому и сетевым ресурсам, при этом разрешая доступ только к некоторым ресурсам. Огороженный сад [walled garden] – это закрытая платформа сетевого сервиса, предоставляемая устройствам и/или пользователям. Находясь внутри огороженного сада, назначенного ТД, мобильные устройства могут иметь доступ только следующим сервисам Протокол Динамической Конфигурации Хоста [Dynamic Host Configuration Protocol (DHCP)], Система Доменных Имен [Domain Name System (DNS)], сервиса push уведомлений, и сервер управления мобильными устройствами [mobile device management (MDM)]. Для того, чтобы выбраться из огороженного сада, мобильное устройство должно найти правильную точку выхода, почти также как в реальном огороженному саду. Назначенная точка выхода для мобильного устройства – это процесс регистрации MDM.
10. С. Оснащение всем необходимым через эфир [Over-the-air provisioning] отличается между разными операционными системами устройств; однако, использование доверенных сертификатов и шифрование Уровня Безопасных Сокетов [Secure Sockets Layer (SSL)] является обычным. Устройства iOS используют Простой Протокол Установки

**1030 Приложение А • Ответы на Контрольные Вопросы**

Сертификатов [Simple Certificate Enrollment Protocol (SCEP)], который использует сертификаты и SSL шифрование для защиты профилей управления мобильными устройствами [mobile device management (MDM)]. Сервер MDM затем посыпает полезную нагрузку SCEP, которая инструктирует мобильное устройство как загрузить доверенные сертификаты с центра сертификации (ЦС) MDM [MDM's certificate authority (CA)] или стороннего ЦС. Как только сертификат установлен на мобильное устройство, зашифрованная полезная нагрузка MDM профиля с настройками устройства и ограничениями безопасно посыпается на мобильное устройство, и устанавливается.

11. A. Обычно IP туннель, использующий Универсальную Маршрутизирующую Инкапсуляцию [Generic Routing Encapsulation (GRE)], может транспортировать гостевой трафик с границы сети внутрь изолированной демилитаризованной зоны [demilitarized zone (DMZ)]. В зависимости от решения производителя БЛВС, назначение туннеля в DMZ может быть контроллер БЛВС, устройство GRE или маршрутизатор. Источник туннеля GRE – это точка доступа (ТД).
12. E. Решение по управлению гостями [guest management solution] с возможностями поручительства сотрудников интегрируется с базой данных Легковесного Протокола Доступа к Каталогу [Lightweight Directory Access Protocol (LDAP)], например Активный Каталог [Active Directory]. От гостевого пользователя может также потребоваться ввод адреса электронной почты сотрудника, который должен подтвердить и поручиться за гостя, прежде чем будет разрешен гостевой доступ к сети. Поручитель [sponsor] обычно получает запрос на доступ для гостя по электронной почте с ссылкой в электронной почте, которая позволяет поручителю легко принять или отказать в запросе. Когда гостевой пользователь зарегистрирован или за него поручились, он может войти со своими только что созданными учетными данными.
13. C. При регистрации своих персональных устройств через корпоративную систему управления мобильными устройствами [mobile device management (MDM)], сотрудники обычно сохраняют возможность удалить профиль MDM, так как это их собственное устройство. Если сотрудник удалит профиль MDM, то устройство больше не управляемся корпоративной системой MDM. Однако, в следующий раз когда сотрудник попытается подключиться к БЛВС компании с мобильного устройства, то он должен будет снова проходить через процесс регистрации в системе MDM.
14. D. Фраза *приноси свое собственное устройство* [*bring your own device (BYOD)*] указывает на политику, разрешающую сотрудникам приносить собственные персональные устройства, такие как смартфоны, планшеты и ноутбуки на свои рабочие места. Политика BYOD указывает какие корпоративные ресурсы могут или не могут быть доступны, когда сотрудники получают доступ в БЛВС компании со своих персональных устройств.
15. A. Логин социальных сетей [Social login] – это метод использования существующих учетных данных входа от социальных сетей, таких как Твиттер [Twitter], Фейсбук [Facebook], или ЛинкедИн [LinkedIn]—чтобы зарегистрировать на стороннем вебсайте. Логин социальных сетей [Social login] позволяет пользователям пропустить процесс создания новых регистрационных учетных записей для стороннего вебсайта. Предприятия розницы и обслуживания понравилась идея логинов социальных сетей, потому что они позволяют им получить значимую маркетинговую информацию о гостевом пользователе из социальной сети. Затем предприятия могут создать базу данных типа заказчиков, которые используют гостевой Wi-Fi во время совершения покупок.
16. F. Мобильное устройство все еще может управляться удаленно, даже если мобильное устройство больше не подключено к корпоративной БЛВС. Сервера управления мобильными устройствами [mobile device management (MDM)] все еще могут управлять устройствами, пока устройства подключены к Интернету в любом месте. Связь между сервером MDM и мобильными устройствами требует уведомления push от сторонних

сервисов. Сервисы push уведомлений посылают сообщение на мобильное устройство, сообщающее устройству, чтобы оно соединилось с MDM сервером. Затем MDM сервер может сделать удаленные действия по защищенному соединению.

17. В, D, E. Изоляция клиентов – это функция, которая может часто быть включены на точках доступа БЛВС или на контроллерах, чтобы заблокировать беспроводных клиентов от связи с другими беспроводными клиентами в том же самом беспроводном VLANe. Изоляция клиентов настоятельно рекомендуется в гостевых БЛВС для предотвращения атак типа равный-с-равным [peer-to-peer attacks]. Производители корпоративных БЛВС также предлагают возможности по сжатию полосы пользовательского трафика Сжатие полосы [Bandwidth throttling], которое также называется ограничение скорости [rate limiting], может быть использовано для обуздания трафика и на уровне идентификатора состава сервиса [service set identifier (SSID)], и на пользовательском уровне. Ограничение скорости трафика гостевых пользователей до 1024кбит/с является обычной практикой. Решение по фильтрации содержимого веб может заблокировать гостевых пользователей от просмотра вебсайтов на основе категории содержимого. Каждая категория содержит вебсайты или веб страницы, которые были туда помещены на основе их преобладающего веб содержания.
18. Е. Перехватывающие порталы доступны как отдельностоящие сервера и как облачные сервисы. Большинство производителей БЛВС предлагают решения интегрированных перехватывающих порталов [integrated captive portal]. Перехватывающий портал может существовать в контроллере БЛВС, или он может быть развернут на границе внутри точки доступа.
19. В. Мобильные устройства должны сначала установить ассоциацию с ТД (точкой доступа). ТД держит мобильное клиентское устройство внутри огороженного сада [walled garden]. Внутри развернутой сети огороженный сад – это закрытая среда, которая ограничивает доступ к веб содержимому и сетевым ресурсам, позволяя при этом доступ к некоторым ресурсам. Огороженный сад является закрытой платформой сетевых сервисов, предоставляемых устройствам и/или пользователям. Пока устройство находится внутри огороженного сада, обозначенного ТД, только эти сервисы могут быть доступны: Динамический Протокол Конфигурации Хостов [Dynamic Host Configuration Protocol (DHCP)], Система Доменных Имен [Domain Name System (DNS)], сервисы push уведомлений, и сервер управления мобильными устройствами [mobile device management (MDM)]. После того, как мобильное устройство завершит процесс регистрации MDM, устройство выпускается из огороженного сада.
20. А, В, С. Сервер контроля доступа к сети [network access control (NAC)] будет использовать информацию о состоянии системы, такую какую показывает агент оценки состояния [posture agent], чтобы определить, что состояние устройства нормальное. Отпечаток Динамического Протокола Конфигурации Хоста [Dynamic Host Configuration Protocol (DHCP)] используется, чтобы помочь идентифицировать оборудование и операционную систему. Атрибуты RADIUS могут быть использованы для идентификации подключен ли клиент беспроводным способом или проводным, вместе с другими параметрами соединения. Изменение Авторизации по RADIUS [RADIUS Change of Authorization (CoA)] используется для отключения или изменения привилегий клиентского соединения.

## Глава 19: 802.11ax: Высокая Эффективность

1. С. Внутри 20 МГц канала максимум девять клиентов может участвовать в многопользовательской OFDMA передаче на каждую возможность передачи [TXOP]. 20 МГц канал может быть поделен на девять отдельных 26-тоновых ресурсных блока.
2. А. Триггерные кадры нужны чтобы осуществлять необходимым обмен кадров для многопользовательской связи. Триггерные кадры используются и для MU-MIMO и MU-OFDMA.
3. В. Целевое время пробуждения [Target wake time (TWT)] – это механизм энергосбережения, изначально определенный в поправке 802.11ah-2016 и улучшенный в 802.11ax. TWT – это обговариваемое соглашение, на основе ожидаемой активности трафика между клиентами и ТД, чтобы определить запланированное время целевого пробуждения для клиентов в режиме энергосбережения [power-save (PS) mode]. Расширенные возможности энергосбережения могут быть идеальными для устройств IoT с радиомодулями 802.11ax, которые передают в полосе 2.4 ГГц.
4. С, F. Работа пространственного переиспользования [Spatial reuse operation (SRO)] позволяет радиомодулям Wi-Fi 6 применять адаптивные пороги обнаружения сигнала в оценке чистоты канала [clear channel assessment (CCA)]. На основе обнаруженного цвета BSS [BSS color] радиомодули Wi-Fi 6 могут применить адаптивную реализацию оценки чистого канала [CCA], которая может поднять порог обнаружения сигнала для меж-BSS кадров [inter-BSS frames], продолжая поддерживать более низкие уровни для внутри-BSS трафика. Если порог обнаружения сигнала поднят выше для входящих OBSS кадров, радиомодулю может не понадобиться откладывать передачу, несмотря на тот же самый канал.
5. С. Хотя первичная цель 802.11ax – это увеличенная эффективность, больше скорости – не плохая вещь. Поднятая эффективность и больше скорости не взаимоисключающие цели. Радиомодули Wi-Fi 6 поддерживают 1024-QAM и новые схемы кодирования и модуляции [modulation and coding schemes (MCSs)], которые определяют более высокие скорости передачи данных.
6. Д. По умолчанию, 1024-QAM используется с 242-поднесущими ресурсными блоками [resource units (RUs)]. Это означает, что по крайней мере все 20 МГц ширины полосы канала обычно будут нужны для 1024-QAM. Более мелкие RU могут быть использованы для 1024-QAM, но радиомодули должны будут поддерживать такую возможность.
7. В, Е. 802.11ax определяет использование обеих многопользовательских технологий, OFDMA и MU-MIMO. Но, пожалуйста, не *перепутайте* OFDMA с MU-MIMO. OFDMA разрешает многопользовательский доступ путем разделения канала. MU-MIMO разрешает многопользовательский доступ путем использования разных пространственных потоков.
8. Д. 802.11ax OFDMA представила более длинное символьное время OFDM в 12.8 микросекунды, которое в четыре раза длиннее, чем старое символьное время в 3.2 микросекунды. В результате более длинного символьного времени, размер поднесущей и пространства уменьшается с 312.5 кГц до 78.125 кГц. Узкое пространство поднесущих обеспечивает лучшее выравнивание и улучшенную канальную надежность. Благодаря 78.125 кГц пространству, 20 МГц OFDMA канал суммарно состоит из 356 поднесущих (тонов).
9. В. Wi-Fi 6 представил многотрафиковый идентификатор агрегированного блока данных MAC протокола (multi-TID AMPDU), который позволяет агрегацию кадров от нескольких идентификаторов трафика [multiple traffic identifiers (TIDs)], из одной и той же или разных категорий доступа QoS. Возможность смешивать MPDUs трафика разных классов QoS позволила радиомодулям Wi-Fi 6 агрегировать более эффективно, уменьшая

служебную информацию [overhead] и, таким образом, увеличивая пропускную способность, и, следовательно, общую сетевую эффективность.

10. В, С, D. В отличие от радиомодулей 802.11ac, которые могут передавать только в полосе частот 5 ГГц, радиомодули 802.11ax могут работать и в 2.4 ГГц и 5 ГГц полосах частот. Когда частотный спектр станет доступным, технология 802.11 ax может также быть использована в полосе 6 ГГц.
11. D. Wi-Fi Альянс обязывает поддерживать DL-OFDMA, UL-OFDMA, и MU- MIMO в нисходящем канале связи. Все первые поколения радиомодулей Wi-Fi 6 поддерживают все три многопользовательские технологии. Поддержка MU-MIMO в восходящем канале может быть в поздних поколениях оборудования Wi-Fi 6; однако, поддержка, для MU-MIMO в восходящем канале будет опционально.
12. A, C. Если в среде присутствуют устаревшие клиенты, ТД Wi-Fi 6 может посыпать многопользовательский кадр запрос-на- отправку [multi-user request- to-send (MU-RTS) frame], который работает как триггерный кадр. Процесс RTS/CTS используется для резервирования среды для OFDMA связи и информирования устаревших клиентов OFDM переустановить свои таймеры NAV на значение равное длительности обмена кадров OFDMA. ТД использует MU-RTS в качестве триггерного кадра, чтобы занять ресурсные блоки [resource units (RUs)] для клиентов, поддерживающих Wi-Fi 6. Клиенты 802.11ax отправят CTS ответы параллельно, используя свои назначенные ресурсные блоки [RU].
13. B. HE MU – это формат заголовка многопользовательского [multi-user] физического уровня (PHY) высокой эффективности [high efficiency], используемой для передачи одному или более пользователям. Этот формат не используется в качестве ответа на триггер, что означает что этот формат заголовка PHY используется для триггерных кадров или передач в нисходящем канале связи.
14. D. Радиомодули Wi-Fi 6 используют три различных защитный интервала, которые могут быть использованы вместе с символьным временем 12.8 мкс, которое используется для модулированных данных: 0.8 мкс, 1.8 мкс, и 3.2 мкс. Защитный интервал 3.2 мкс предназначен для связи вне помещений. При комбинации с временем 12.8 мкс, которое используется для данных, общее символьное время будет 16.0 мкс. Более длинное символьное время и более длинные защитные интервалы обеспечивают более надежную связь вне помещений.
15. D. Очень хорошее применение для MU-MIMO – это канал связи мост точка-многоточка [point-to-multipoint (PtMP)] между зданиями. Пространственное разнесение, которое требуется для MU-MIMO, присутствует в этом типе установки вне помещений. Каналы-мосты требуют высокую ширину полосы, которую может MU-MIMO предоставить в установке PtMP.
16. B. 802.11ax определяет процедуру индикации режима работы [operating mode indication (OMI)] для этой цели. Клиент может переключаться между однопользовательской или многопользовательской UL-OFDMA работой с изменением в режиме работы по передаче [transmit operating mode (TOM)]. Следовательно, клиент Wi-Fi 6 может и прекращать, и возобновлять отвечать на триггерные кадры, отправленные ТД во время процесса UL- OFDMA.
17. D. Вероятно наиболее важная беседа о связи между коммутаторами и ТД Wi-Fi 6 – это требования к Питанию по Ethernet [Power over Ethernet (PoE)]. 15.4 ватт (Вт) выдаваемые на порт по стандарту 802.11af PoE будет недостаточно для большинства ТД 4×4:4, и следовательно, будет необходимо питание 802.3at (PoE Plus). Коммутаторы с поддержкой PoE Plus могут предоставить до 30 ватт питания на

Ethernet порт. Порты с питанием PoE Plus для ТД 4×4:4 и 8×8:8 должны считаться стандартным требованием.

18. A. UL-OFDMA требует использование кадров отчетов о состоянии буфера [buffer status report (BSR) frames] от клиентов. Клиенты используют кадры BSR для уведомления ТД о забуферизированных клиентских данных и о категории QoS данных. Информация, содержащаяся в кадрах BSR, помогает ТД в выделении RUs для синхронизированной передачи в восходящем канале связи. ТД будет использовать информацию, собранную от клиентов, чтобы построить окна времени для восходящей связи [uplink window times], выделение клиентских RU [client RU allocation], и настройки клиентского электропитания для каждого RU. BSRs могут быть незапрашиваемые или запрашиваемые.
19. A, D, E. При сравнении двух многопользовательских технологий 802.11ax, MU-MIMO и OFDMA, у каждой есть свои собственные преимущества. MU-MIMO – лучше подходит для увеличенной емкости, приложений с широкой полосой пропускания, большими пакетами, и высокой скоростью передачи данных на пользователя. OFDMA лучше подходит для увеличенной эффективности, приложений с низкими полосами пропускания, небольшими пакетами, и задержкой. **20.** С, D. Цвет BSS – это идентификатор базового состава сервиса [basic service set (BSS)]. В реальности, идентификатор цвета BSS не является цветом, а числовым идентификатором. Радиомодули Wi-Fi способны различать между BSS, использующими BSS цвет (численный идентификатор), когда другие радиомодули передают на одном и том же канале.

## Глава 20: Установка БЛВС и Вертикальные Рынки

1. A, B, C, D. Радиомодули Wi-Fi используются в сенсорах и мониторивых устройствах IoT, так же как RFID, в многочисленных вертикальных ранках предприятий. Устройства IoT часто используют другие беспроводные сетевые технологии, такие как Bluetooth, Zigbee, и Z-Wave, вместо беспроводной технологии 802.11. Устройства IoT могут также подключаться к корпоративной сети через Ethernet.
2. B. Радиомодуль iBeacon BLE передает местоположение зоны непосредственной близости в виде универсального уникального идентификатора [universally unique identifier (UUID)], с главным числом и второстепенным числом. UUID – это 32-символьная шестнадцатеричная строка, которая уникально определяет организацию, под управлением которой находятся маяки. UUID включен в полезную нагрузку iBeacon с главным и второстепенным числами, которые обычно показывают определенное место и положение в этом месте, соответственно.
3. C. Из-за потенциальной интерференции и важности ее предотвращения, в больницах часто есть персона, отвечающая за отслеживание используемых внутри организации частот. Некоторые муниципалитеты начали поступать так же-не только для усиления соблюдения закона, но и для всех своих беспроводных нужд, так как они часто используют беспроводные технологии для сетей АСУ ТП [SCADA], камер наблюдения, светофор, двунаправленная радиосвязь, мосты точка-точка, хотспоты и т.д. На военных базах также обычно есть человек, отвечающий за управление спектром.
4. D. Поскольку круизные корабли часто находятся не около земли, где доступен канал сотового LTE, то необходимо использовать спутниковый канал для подключения корабля к Интернету.

5. В, D. Сходимость фиксированной и мобильной связи [Fixed mobile convergence] позволяет переключаться между Wi-Fi сетями и сетями сотовой телефонии, выбирая доступную сеть, которая наименее дорогая.
6. D. При проектировании сети склада, сетевыми устройствами часто являются сканеры штрих-кодов, которые не записывают много данных, потому высокая емкость и пропускная способность обычно не являются приоритетными. Из-за того, что требования к передаче данных такие низкие, эти сети обычно спроектированы для обеспечения покрытия больших площадей. Безопасность всегда является вопросом; однако, обычно это не является критерием проектирования.
7. D. Годами стоял вопрос о неблагоприятном влиянии на здоровье от влияния радиоволн на людей и животных. Всемирная Организация Здравоохранения [World Health Organization] сделала заключение, что нет убедительных научных доказательств, что слабые радиочастотные сигналы, такие как в связи 802.11, вызывают неблагоприятное влияние на здоровье. Бобу следует направить сомневающихся людей на отчеты о медицинских исследованиях, доступных у Wi-Fi Альянсе и Всемирной Организации Здравоохранения.
8. С. Растиущая тенденция в отрасли информационных технологий (IT) для компаний переключаться на провайдеров управляемых услуг [managed services provider (MSP)]. Небольшие и среднего размера предприятия [Small and medium-sized businesses (SMBs)] и крупные предприятия мигрируют управление и мониторинг на облачных MSP.
9. В. Хотя все эти ответы верные, главное назначение сетей малого офиса/домашнего офиса [small office/home office (SOHO)] в предоставлении шлюза в Интернет.
10. А. Производители БЛВС предлагают эффективное по стоимости решение для сотрудников на удаленке [teleworkers] для доступа к корпоративным ресурсам через IPsec VPN 2ого уровня безопасно с помощью точки доступа компании. Удаленная ТД уровня предприятия работает как конечная точка VPN 2ого уровня дома у удаленного сотрудника, и может быть автоматически оснащена через систему управления сетью [network management system (NMS)].
11. А, D. Складские и производственные среды обычно нужна мобильность, но данных для передачи обычно очень мало. Следовательно, такие сети часто проектируются для широко покрытия, а не для высокой емкости.
12. В, C. iBeacons требует приложение на мобильном устройстве, чтобы запустить действие. Запуск происходит, когда смартфон с приемным радиомодулем BLE находится в близкой зоне действия передатчика iBeacon. Например, iBeacon может запустить push уведомления в зонах непосредственной близости таких, как реклама в местах розничной продажи. iBeacons использует радиомодули BLE, а не радиомодули 802.11; однако, многие производители БЛВС теперь предлагают интегрированные и/или устанавливаемые поверх решения технологии iBeacon. Не перепутайте iBeacons, используемый передатчиками BLE, с кадрами управления 802.11 – маяками [beacon], которые передаются Wi-Fi точками доступа.
13. А, В, С. Производственный завод – это обычно фиксированная среда и лучше обслуживается постоянными точками доступа.
14. С, D. Точка-многоточка [Point-to-multipoint], ступица и спицы [hub and spoke], и звезда [star] – все описывают одну и ту же технологию связи, которая соединяет несколько устройств с помощью центрального устройства. Связь точка-точка [Point-to-point] соединяет два устройства. Взаимосвязанные [Mesh] сети не определяют центрального устройства.
15. С. Most Большинство исходных установок 802.11 использовали расширение спектра с перестройкой частоты [frequency-hopping spread spectrum (FHSS)], промышленные (складские и производственные) компании являются одними из самых больших кто установил их. Их требования к мобильности с низкими скоростями передачи данных были

**1036      Приложение А • Ответы на Контрольные Вопросы**

идеальны для использования этой технологии. Даже если технологии 20 лет, все ещё сохранились некоторые установки.

- 16.** С. Чтобы сделать беспроводной доступ легким для абонентов, производители хотспотов обычно разворачивают методы аутентификации, которые просты в использовании, но которые не предоставляют шифрование данных. Следовательно, чтобы гарантировать безопасность до вашей корпоративной сети, наиболее часто необходимо использование IPsec VPN.
- 17.** А, С, D. Голос поверх Wi-Fi [Voice over Wi-Fi (VoWiFi)] – типовое использование технологии 802.11 в медицинской среде, обеспечивающее немедленный доступ к персоналу в независимости от того, где он находится в больнице. Решения Сервисов Определения местоположения в Реальном Времени [Real-time location service (RTLS)] с помощью меток 802.11 RFID для контроля инвентаря также является обычной практикой. Беспроводные медицинские карты [WLAN medical carts] используются для мониторинга информации о пациенте и жизненных параметров.
- 18.** А, С. Установка двух мостов точка-точка или для предоставления более высокой пропускной способности, или для предотвращения единой точки отказа путем предоставления резервирования. Требует соблюдать осторожность при организации канала и установки антенн, чтобы избежать интерференции от самих себя.
- 19.** А, В, С, D. Так как у организаций здравоохранения много устройств, которые используют радиосвязь, то радиоинтерференция – это вопрос. Быстрый, безопасный и точный доступ является критичным в среде здравоохранения. Мобильность технологий удовлетворит более быстрый доступ, чем обычно требуется.
- 20.** С. Решения филиальных маршрутизаторов обычно применяет IPsec VPN 3его уровня и использует возможность внутреннего DHCP вместе с NAT для предоставления локальной IP связности. Решение IPsec VPN 2ого уровня обычно используется с удаленными ТД. IP подключение удаленного сотрудника [Teleworker] обычно предоставляется DHCP сервером из корпоративной штаб-квартиры.