

Компьютерные системы и сети

Выпуск 2

Компьютерные системы и сети

Серия основана в 2013 году

Ответственный редактор А.В. Пролетарский

РЕДАКЦИОННЫЙ СОВЕТ:

А.А. Александров (*председатель*), д-р техн. наук
В.А. Матвеев (*гл. редактор*), д-р техн. наук
В.В. Девятков, д-р техн. наук
И.П. Иванов, д-р техн. наук
А.П. Карпенко, д-р техн. наук
Е.А. Микрин, академик РАН
А.В. Пролетарский, д-р техн. наук
И.В. Рудаков, канд. техн. наук
В.В. Сюезев, д-р техн. наук
В.М. Черненький, д-р техн. наук
В.А. Шахнов, член-корр. РАН

Москва
Издательство МГТУ им. Н.Э. Баумана
2017

Технологии современных беспроводных сетей Wi-Fi

Под общей редакцией А.В. Пролетарского

Допущено Федеральным учебно-методическим объединением в системе высшего образования по укрупненной группе специальностей и направлений подготовки 09.00.00 «Информатика и вычислительная техника» в качестве учебного пособия для студентов (адъюнктов), обучающихся по основным образовательным программам высшего образования по направлениям подготовки бакалавриата/магистратуры укрупненной группы специальностей и направлений подготовки 09.00.00 «Информатика и вычислительная техника»



МОСКВА
ИЗДАТЕЛЬСТВО
МГТУ им. Н.Э. БАУМАНА
2017

УДК 004.7
ББК 32.973.202
Т38

А в т о р ы:
Е.В. Смирнова, А.В. Пролетарский, Е.А. Ромашкина,
С.А. Балюк, А.М. Суоров

Р е ц е н з е н т ы:
генеральный директор АО «РтСофт», д-р техн. наук *О.В. Синенко*;
директор фирмы «1С», канд. экон. наук *Б.Г. Нуралиев*

Т38 **Технологии современных беспроводных сетей Wi-Fi** : учебное пособие / [Е. В. Смирнова, А. В. Пролетарский и др.] ; под общ. ред. А. В. Пролетарского. — Москва : Издательство МГТУ им. Н.Э. Баумана, 2017. — 446, [2] с. : ил. — (Компьютерные системы и сети).

ISBN 978-5-7038-4620-9

Изложены основные сведения о современных технологиях беспроводных сетей Wi-Fi и показано поэтапное проектирование беспроводных сетей — от планирования производительности и зоны действия до развертывания и тестирования сети. Подробно рассмотрен стандарт IEEE 802.11, включая управление доступом к среде, а также физический уровень 802.11. Описаны особенности радиочастотного спектра, принципы модуляции, приведены варианты спецификаций 802.11, технологии повышения производительности и механизмы защиты. Подробно рассмотрено подключение клиента к беспроводной сети в инфраструктурном режиме — сканирование, методы аутентификации и ассоциации, а также вопросы безопасности передачи данных в беспроводных сетях (WEP, TKIP, CCMP, WPA, WPA2, WPS). Приведены оценка беспроводной линии связи и пример расчета. Представленные в учебном пособии теоретические положения дополнены лабораторными работами по всем рассмотренным в книге темам. Издание содержит обширный глоссарий.

Учебное пособие подготовлено сотрудниками компании D-Link и преподавателями МГТУ имени Н.Э. Баумана. Содержание соответствует курсу лекций, который авторы читают в МГТУ имени Н.Э. Баумана и совместном центре «МГТУ — D-Link».

Для студентов высших учебных заведений, обучающихся по основным образовательным программам высшего образования по направлениям подготовки бакалавриата/магистратуры укрупненной группы специальностей и направлений подготовки «Информатика и вычислительная техника».

УДК 004.7
ББК 32.973.202



Все права защищены. Никакая часть данного издания не может быть воспроизведена в какой бы то ни было форме без письменного разрешения владельцев авторских прав. Правовую поддержку Издательства обеспечивает Адвокатское бюро «Сергей Москаленко и партнеры».

ISBN 978-5-7038-4620-9

© Оформление. Издательство
МГТУ им. Н.Э. Баумана, 2017

Оглавление

Предисловие	8
Обозначения, используемые в книге	11
1. Технологии беспроводных сетей	12
1.1 Что такое Wi-Fi?	12
1.2. Основные устройства беспроводных сетей	13
1.2.1. Клиентские устройства	13
1.2.2. Точки доступа	15
1.2.3. Беспроводные маршрутизаторы	18
1.2.4. Беспроводные повторители	20
1.2.5. Беспроводные мосты	21
1.2.6. Антенны	22
1.3. Преобразование единиц измерения	43
2. Стандарт беспроводных локальных сетей IEEE 802.11	46
2.1. Архитектура IEEE 802.11	46
2.2. Услуги IEEE 802.11	54
2.2.1. Распределение сообщений в пределах распределительной системы	55
2.2.2. Услуги, связанные с ассоциацией	56
2.2.3. Услуги управления доступом и обеспечения безопасности	57
2.3. Кадр MAC стандарта IEEE 802.11	59
2.4. Управление доступом к среде в стандарте IEEE 802.11	63
2.4.1. Функция распределенной координации (DCF)	65
2.4.2. Функция точечной координации (PCF)	74
2.4.3. Понятие QoS	76
2.4.4. Функция гибридной координации (HCF)	77
2.4.5. Программа сертификации Wi-Fi Multimedia (WMM)	81
2.4.6. Фрагментация кадров в беспроводной сети	82
3. Подключение клиента к беспроводной сети в инфраструктурном режиме	84
3.1. Сканирование	85
3.2. Аутентификация и ассоциация	88
3.2.1. Аутентификация 802.11	90
3.2.2. Ассоциация после аутентификации 802.11	94
3.3. Аутентификация RSN и безопасная ассоциация	95
3.3.1. Аутентификация на основе стандарта IEEE 802.1X	95
3.3.2. Аутентификация на основе предварительно установленных ключей (PSK)	101
3.4. Дополнительные методы контроля доступа к беспроводной сети	102
4. Безопасность передачи данных в беспроводных сетях	104
4.1. Протокол WEP	104
4.2. Протокол TKIP	106
4.3. Протокол CCMP	109
4.4. Программы сертификации WPA/WPA2	112
4.5. Программа сертификации Wi-Fi Protected Setup (WPS)	115
5. Физический уровень стандарта IEEE 802.11	120
5.1. Особенности использования радиочастотного спектра	122
5.2. Технологии модуляции физического уровня IEEE 802.11	124
5.2.1. Технологии расширения спектра	124
5.2.2. Мультиплексирование с ортогональным частотным разделением	129
5.3. Спецификация IEEE 802.11a	134
5.4. Спецификация IEEE 802.11b	135
5.5. Спецификация IEEE 802.11g	137

5.6. Спецификация IEEE 802.11n	138
5.6.1. Технологии повышения производительности на физическом уровне 802.11n	139
5.6.2. Совместимость со спецификациями 802.11a/b/g	160
5.6.3. Структура физического интерфейса 802.11n	162
5.6.4. Технологии повышения производительности на MAC-подуровне 802.11n	165
5.6.5. Механизмы защиты 802.11n при работе в сети с устройствами 802.11a/b/g	168
5.6.6. Механизмы сосуществования при использовании каналов 20/40 МГц	172
5.7. Спецификация IEEE 802.11ac	174
5.7.1. Технологии физического уровня 802.11ac	176
5.7.2. Технологии повышения производительности на MAC-подуровне 802.11ac	188
5.7.3. Механизмы защиты и сосуществования при работе в сети с устройствами 802.11a/n	189
5.7.4. Downlink Multi-User MIMO	192
5.7.5. Выход оборудования 802.11ac на рынок	196
6. Оценка беспроводной линии связи	197
6.1. Общие сведения	197
6.2. Пример расчета линии связи	209
7. Проектирование беспроводных сетей	212
7.1. Этапы проектирования беспроводной сети	213
7.2. Сбор информации о клиентских устройствах	214
7.3. Планирование производительности и зоны охвата беспроводной сети	216
7.3.1. Скорость передачи данных и пропускная способность	217
7.3.2. Скорость передачи данных и дальность действия беспроводной сети	223
7.3.3. Выбор частотного диапазона	225
7.3.4. Настройка мощности передатчика	226
7.3.5. Использование антенн	227
7.3.6. Выбор радиочастотного канала	228
7.4. Предпроектное обследование места развертывания беспроводной сети	235
7.4.1. Моделирование зоны покрытия беспроводной сети внутри помещения	236
7.4.2. Обследование помещения	243
7.5. Постпроектное обследование и тестирование сети	245
8. Развертывание беспроводной сети	247
8.1. Проблемы при развертывании больших беспроводных сетей	247
8.2. Архитектуры беспроводных сетей	248
8.2.1. Автономная архитектура беспроводной сети	248
8.2.2. Централизованная архитектура беспроводной сети	250
8.2.3. Распределенная архитектура беспроводной сети	252
8.3. Беспроводная распределительная система (WDS)	253
8.3.1. Топологии WDS-сетей	255
8.3.2. Настройка WDS-соединений	258
8.4. Обеспечение отказоустойчивости в беспроводных сетях	266
8.5. Режимы работы точек доступа	268
8.6. Организация электропитания точек доступа	270
8.7. Сегментация беспроводной сети	271
8.8. Настройка QoS	287
8.9. Функции оптимизации производительности	290
8.10. Функции безопасности	293
8.10.1. Аутентификация и конфиденциальность данных	293
8.10.2. Виртуальные частные сети (VPN)	296
8.10.3. Защита от вторжений	297
8.11. Роуминг	301

8.12. Функции настройки и управления	306
8.12.1. Технология AP Array	306
8.12.2. Технология кластеризации точек доступа	309
8.12.3. Управление точками доступа с использованием аппаратного беспроводного контроллера	311
8.12.4. Программный контроллер D-Link Central WiFiManager	312
Лабораторные работы по курсу «Технологии современных беспроводных сетей Wi-Fi» ...	316
Рекомендации по организации лабораторных работ	316
<i>Лабораторная работа № 1. Преобразование единиц измерения в беспроводных сетях</i>	<i>317</i>
<i>Лабораторная работа № 2. Создание беспроводной сети в инфраструктурном режиме</i>	<i>320</i>
2.1. Установка драйвера беспроводного сетевого адаптера	321
2.2. Настройка точки доступа в режиме Access Point	325
2.3. Мониторинг беспроводных сетей с помощью программы <i>inSSIDer Home</i>	332
2.4. Настройка точки доступа в режиме Wireless Client	334
2.5. Настройка точки доступа в режиме AP Repeater	336
<i>Лабораторная работа № 3. Объединение инфраструктурных BSS с единым SSID через распределительную систему</i>	<i>338</i>
3.1. Изменение IP-адреса управления точек доступа AP1 и AP2	339
3.2. Настройка точки доступа AP1	340
3.3. Настройка точки доступа AP2	340
3.4. Проверка работоспособности схемы	340
<i>Лабораторная работа № 4. Исследование кадров MAC стандарта IEEE 802.11</i>	<i>342</i>
4.1. Захват трафика с помощью сетевого анализатора Microsoft Network Monitor	345
4.2. Анализ кадров MAC стандарта IEEE 802.11	350
<i>Лабораторная работа № 5. Изучение пассивного и активного сканирования</i>	<i>358</i>
<i>Лабораторная работа № 6. Обеспечение безопасности в беспроводных сетях</i>	<i>362</i>
6.1. Настройка режима WPA/WPA2-Personal	363
6.2. Контроль доступа к беспроводной сети на основе MAC-адресов	367
<i>Лабораторная работа № 7. Расчет беспроводной линии связи</i>	<i>369</i>
7.1. Примеры расчета беспроводной линии связи	372
7.2. Задания для самостоятельного выполнения	375
<i>Лабораторная работа № 8. Влияние скорости передачи на производительность и дальность действия сети</i>	<i>376</i>
8.1. Оценка производительности беспроводной сети	377
8.2. Оценка зависимости скорости передачи от дальности действия сети	381
8.3. Применение антенны с высоким коэффициентом усиления	382
<i>Лабораторная работа № 9. Настройка распределенной сети (WDS)</i>	<i>383</i>
9.1. Настройка WDS-соединения типа «точка—точка»	384
9.2. Настройка WDS-соединения типа «точка—много точек»	388
<i>Лабораторная работа № 10. Настройка сегментации сети</i>	<i>392</i>
10.1. Настройка сегментации проводной и беспроводной сети	393
10.2. Настройка сегментации распределенной сети	403
<i>Лабораторная работа № 11. Настройка функции AP Array</i>	<i>408</i>
<i>Лабораторная работа № 12. Сегментация беспроводной сети на основе двухдиапазонных точек доступа</i>	<i>415</i>
<i>Лабораторная работа № 13. Настройка программного контроллера CWM-100</i>	<i>423</i>
Литература	433
Глоссарий	434

Предисловие

Развитие цивилизации можно проследить на примере изменения технологий работы с информацией. Если речь идет о хранении информации, то от наскальных рисунков до облачных хранилищ, если о скорости обработки информации, то от счетов до суперЭВМ, если о методах передачи информации, то от жестов до беспроводной связи.

История беспроводных технологий передачи информации началась в конце XIX века с передачи первого радиосигнала и появления в 1920-х годах первых радиоприемников с амплитудной модуляцией. В 1930-е годы появилось радио с частотной модуляцией и телевидение, в 1970-е годы созданы первые беспроводные телефонные системы как результат удовлетворения потребности в мобильной передаче голоса. Сначала это были аналоговые сети, а начале 1980-х был разработан стандарт GSM, ознаменовавший начало перехода на цифровые стандарты, обеспечивающие лучшее распределение спектра, качество сигнала и безопасность. С 1990-х годов происходит укрепление позиций беспроводных сетей и беспроводные технологии прочно входят в нашу жизнь. Интенсивно развиваясь, они приводят к созданию новых устройств и услуг, повышают качество жизни.

Обилие беспроводных технологий, таких, как CDMA (*Code Division Multiple Access* — технология с кодовым разделением каналов), GSM (*Global for Mobile Communications* — глобальная система для мобильных коммуникаций), EDGE (*Enhanced Data Rates for GSM Evolution* — увеличенная скорость передачи данных для GSM), 3G (третье поколение), LTE (*Long-Term Evolution*, 4G), 5G, TDMA (*Time Division Multiple Access* — множественный доступ с разделением во времени), WAP (*Wireless Application Protocol* — протокол беспроводных технологий), IEEE 802.11, GPRS (*General Packet Radio Service* — услуга пакетной передачи данных), Bluetooth (голубой зуб, по имени Харальда Голубого Зуба — предводителя викингов, жившего в X веке — компромисс между экономичностью, дальностью и скоростью), ZigBee (минимальное энергопотребление), 434/868 МГц (максимальная дальность в прямой видимости), NFC (*Near Field Communication* — малый радиус действия) и т. д., говорит о том, что в этой области происходит революция.

Весьма перспективно развитие и беспроводных локальных сетей (WLAN), Bluetooth (сети средних и коротких расстояний). Беспроводные сети развертываются в аэропортах, университетах, отелях, ресторанах, на предприятиях. История разработки стандартов беспроводных сетей началась в 1990 году, когда международной некоммерческой ассоциацией IEEE (Institute of Electrical and Electronics Engineers — Институт инженеров электротехники и электроники) был образован комитет 802.11. Значительный импульс развитию беспроводных технологий дала «Всемирная паутина» и идея работы в сети при помощи беспроводных устройств. В конце 1990-х годов пользователям была предложена WAP-услуга, сначала не вызвавшая у населения большого интереса и представляющая собой основные информационные услуги —

новости, погода, всевозможные расписания и т. п. Также весьма низким спросом пользовались вначале и Bluetooth, и WLAN в основном из-за высокой стоимости этих средств связи. Однако по мере снижения цен рос интерес населения. К середине первого десятилетия XXI века счет пользователей беспроводного интернет-сервиса пошел на десятки миллионов. С появлением беспроводной интернет-связи на первый план вышли вопросы обеспечения безопасности. Основные проблемы при использовании беспроводных сетей — это перехват сообщений спецслужб, коммерческих предприятий и частных лиц, перехват номеров кредитных карточек, кража оплаченного времени соединения, вмешательство в работу коммуникационных центров. Эти проблемы решаются путем усовершенствования стандартов связи.

Существенным для развития беспроводных технологий является и возможность их использования домашними пользователями. С ростом числа устройств в домашней сети все более актуальной становится проблема множества проводов, соединяющих эти устройства между собой, а это уже повод для перехода на беспроводные технологии. Повышение степени комфортности современного дома, объединение в единое целое всех его структур и объектов (компьютеров, телевизоров, цифровых фотокамер, домашнего развлекательного центра, систем охраны, климатических систем, кухонных устройств и т. д.) — основа идеи создания интеллектуального цифрового дома — также реализуется с помощью беспроводных устройств.

Важную роль беспроводные технологии играют и в концепции «интернета вещей», определяющей принципы взаимодействия физических предметов между собой и с внешним окружением.

Хотя насчитывается огромное число единичных пользователей, быстрорастущим сегментом потребителей беспроводных технологий является корпоративный. Беспроводная передача данных — важное стратегическое средство, обеспечивающее рост производительности (сотрудники получают постоянный и быстрый доступ к корпоративной информации, быстрее узнают новости), повышающее качество обслуживания клиентов (можно мгновенно принимать жалобы и пожелания и оперативно реагировать на них), создающее конкурентные преимущества (повышение скорости обмена информацией и, следовательно, скорости принятия решения). Ну а в будущем нас ждет беспроводной цифровой мир.

В учебном пособии рассмотрены теоретические и практические вопросы, связанные с созданием беспроводных сетей и устройств, их реализующих. В основу пособия легли материалы занятий, проводимых в авторизованном учебном центре «МГТУ — D-Link», созданном в 2006 году для продвижения современных сетевых технологий. Центр объединил фундаментальное образование в области информационных технологий от МГТУ им. Н.Э. Баумана с практическими знаниями от компании D-Link.

В главе 1 рассматриваются технологии создания беспроводных сетей и устройства для их реализации.

Глава 2 посвящена подробному изучению стандарта IEEE 802.11, включая управление доступом к среде.

В главе 3 изложены вопросы подключения клиента к беспроводной сети в инфраструктурном режиме — сканирование, методы аутентификации и ассоциаций.

Глава 4 посвящена вопросам безопасности передачи данных в беспроводных сетях (WEP, TKIP, CCMP, WPA, WPA2, WPS).

В главе 5 всесторонне рассматривается физический уровень 802.11. Показаны особенности радиочастотного спектра, принципы модуляции, даны варианты спецификаций 802.11, описаны технологии повышения производительности, механизмы защиты.

В главе 6 проводится оценка беспроводной линии связи и приведен пример ее расчета.

Главы 7 и 8 включают вопросы поэтапного проектирования беспроводных сетей: от планирования производительности и зоны действия до развертывания и тестирования сети.

Практическая часть учебного пособия состоит из 13 лабораторных работ, включающих изучение и настройку основных параметров точек доступа и беспроводных маршрутизаторов, функций безопасности, сегментации беспроводной сети, средств управления и мониторинга. Отдельные лабораторные работы посвящены преобразованию единиц измерения и расчету беспроводной линии связи. Кроме того, две последние работы включают изучение и настройку сегментации беспроводной сети на основе частотных диапазонов и SSID/VLAN, а также настройку точек доступа с помощью программного контроллера Central WiFiManager.

Издание снабжено обширным глоссарием.

Обозначения, используемые в книге

В тексте книги используются следующие пиктограммы для обозначения сетевых устройств различных типов:



Коммутатор



Беспроводной контроллер



Маршрутизатор



Точка доступа



Беспроводной маршрутизатор



Рабочая станция



Ноутбук



Персональный компьютер



Сервер



Принтер



Сетевая среда



Беспроводная среда



Смартфон



Телевизор



Пользователь



Станция управления сетью



Беспроводной повторитель



Беспроводной мост



IP-камера

1. Технологии беспроводных сетей

1.1 Что такое Wi-Fi?

Термин *Wi-Fi* не является техническим, но активно применяется современными пользователями. Под аббревиатурой *Wi-Fi* (от английского словосочетания *Wireless Fidelity*, которое можно дословно перевести как *высокая точность беспроводной передачи данных*) в настоящее время понимается целое семейство стандартов передачи цифровых потоков данных по радиоканалам. Другими словами, под термином Wi-Fi пользователи подразумевают технологии беспроводных локальных сетей — *Wireless Local Area Network (WLAN, Wireless LAN)*. Эти технологии позволяют объединять компьютеры в локальные сети без помощи проводов (т. е. используя радиоволны) и подключать их к Интернету.

Наиболее правильное определение термина Wi-Fi — это торговая марка консорциума Wi-Fi Alliance — объединения крупнейших производителей компьютерной техники и беспроводных устройств Wi-Fi. Эта организация курирует коммерческое развитие технологии Wi-Fi на базе стандартов, разработанных и ратифицированных институтом IEEE (группа стандартов 802.11). Одной из задач консорциума является тестирование оборудования различных производителей на предмет совместимости и корректности работы устройств друг с другом.

При полном соответствии оборудования всем предъявляемым Wi-Fi Alliance требованиям производитель может разместить на упаковке информацию о его сертификации (рис. 1.1). Компания D-Link является постоянным членом консорциума Wi-Fi Alliance.



Рис. 1.1. Логотип Wi-Fi Alliance

Беспроводные технологии получают с каждым годом все большее развитие. Уже никого не удивляет наличие сетей Wi-Fi в транспорте, в зонах отдыха, кафе и на вокзалах. Беспроводные сети особенно эффективны на предприятиях, где сотрудники во время рабочего дня активно перемещаются по территории с целью обслуживания клиентов или сбора информации (крупные склады, агентства, офисы продаж,

учреждения здравоохранения и др.).

Беспроводные локальные сети имеют ряд преимуществ перед проводными локальными сетями:

- быстрое развертывание, что очень удобно в условиях работы вне офиса (например, при проведении презентаций);
- легкое перемещение пользователей мобильных устройств при подключении к локальным беспроводным сетям в рамках действующих зон сети без разрыва соединения благодаря функции роуминга между точками доступа;

- использование современных сетей за счет высоких скоростей для решения очень широкого спектра задач;
- простота организации беспроводной локальной сети в случае, когда прокладка кабеля невозможна.

Вместе с тем необходимо помнить об ограничениях беспроводных сетей. Это, как правило, меньшая скорость и расстояние передачи данных по сравнению с проводными сетями, подверженность влиянию помех и более сложная схема обеспечения безопасности передаваемой информации.

Беспроводные сети могут использоваться как самостоятельно, так и входить в состав сетей сложной архитектуры, содержащих как беспроводные, так и проводные сегменты.

Наиболее часто сети Wi-Fi используются для решения следующих задач:

- беспроводное подключение пользователей к проводным сетям;
- объединение пространственно разнесенных подсетей в одну общую сеть там, где кабельное соединение подсетей невозможно или нежелательно;
- подключение пользователей к сетям провайдеров интернет-услуг.

1.2. Основные устройства беспроводных сетей

Для построения беспроводных сетей используются различные типы устройств — беспроводные клиентские устройства, точки доступа, беспроводные маршрутизаторы, повторители, мосты и антенны.

1.2.1. Клиентские устройства

Под беспроводными клиентскими устройствами понимаются устройства со встроенными или подключенными *беспроводными сетевыми адаптерами* (*Wireless Network Interface Card, Wireless NIC*) (рис. 1.2), которые обеспечивают клиентским устройствам интерфейс для подключения к беспроводным сетям.

Беспроводной адаптер может быть:

- встроенным в материнскую плату ноутбука, планшета, смартфона, электронной книги и т. п.;
- внутренним, представляющим собой отдельную плату, устанавливаемую в слот PCI, PCI Express, PCIe компьютера;
- внешним, подключающимся к компьютеру или ноутбуку через интерфейс USB или CardBus (PCMCIA).

Пример архитектуры беспроводного адаптера приведен на рис. 1.3.

Беспроводной адаптер реализует функции MAC-подуровня и соответствующего физического уровня или уровней 802.11 (см. гл. 2): 802.11a, 802.11b, 802.11g, 802.11n или 802.11ac. Существуют адаптеры, работающие как в одном частотном диапазоне 2,4 или 5 ГГц, так и в обоих (*dual-mode*).

Внимание: в стандарте 802.11 клиентские устройства называются станциями 802.11 (иногда используется аббревиатура STA).

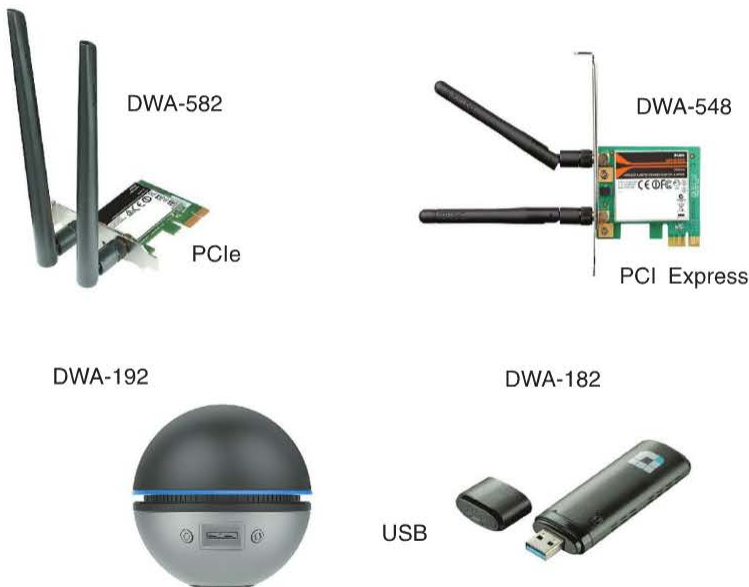


Рис. 1.2. Беспроводные сетевые адаптеры D-Link

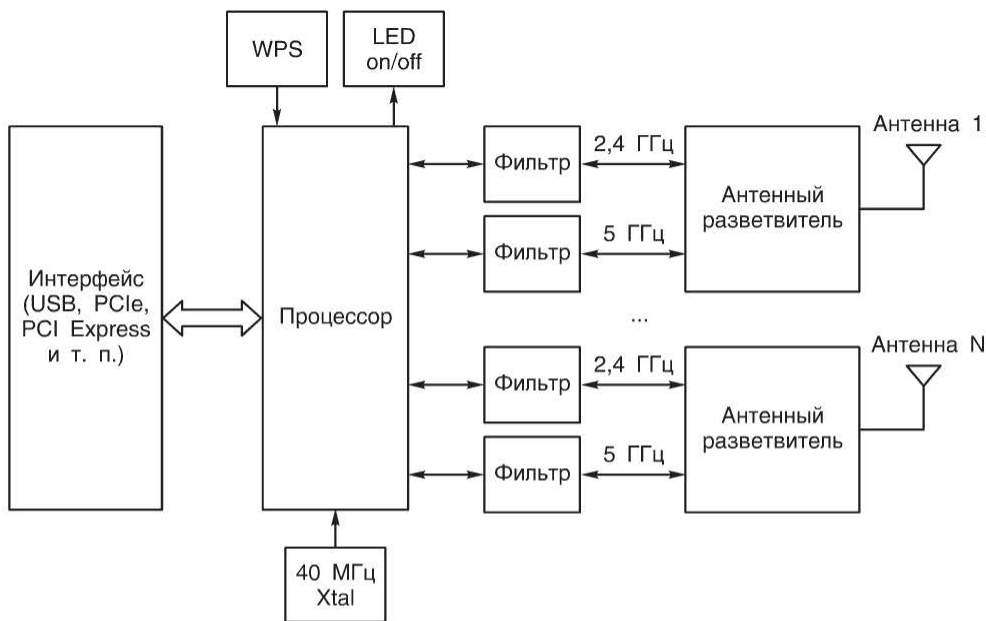


Рис. 1.3. Пример архитектуры беспроводного адаптера

1.2.2. Точки доступа

Точки доступа (*Access Point, AP*) так же, как и беспроводные адаптеры, реализуют функции MAC-подуровня и соответствующего физического уровня или уровней 802.11. Пример архитектуры точки доступа приведен на рис. 1.4.

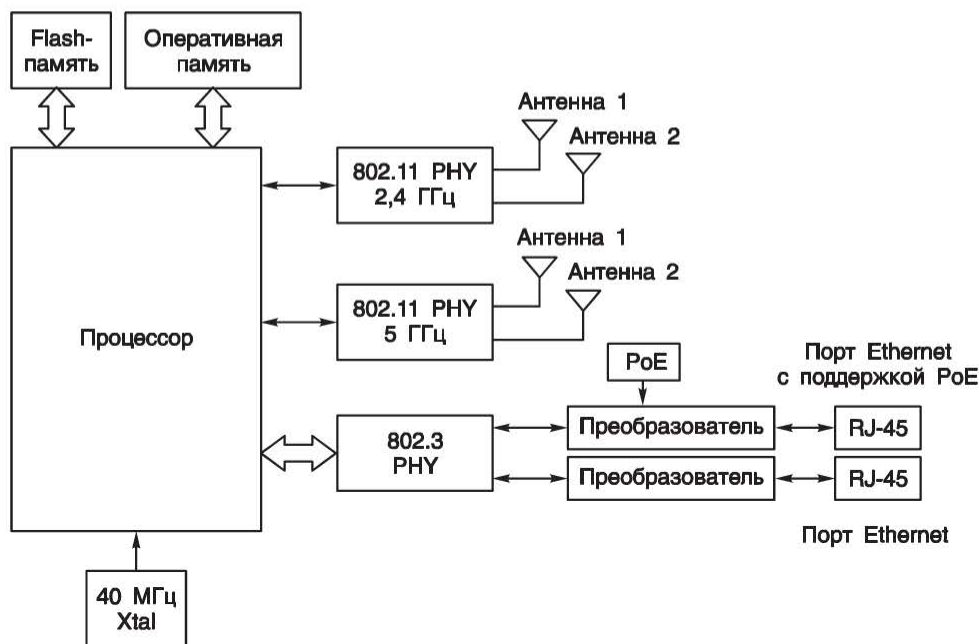


Рис. 1.4. Пример архитектуры точки доступа

Точка доступа (рис. 1.5) является основным компонентом инфраструктуры беспроводной сети. Через нее осуществляется обмен информацией между беспроводными клиентскими устройствами, а также подключение к общей распределительной системе (обычно сети Ethernet), для чего у точки доступа имеется сетевой интерфейс Ethernet (uplink port) с разъемом 8P8C (RJ-45). Через этот же интерфейс может осуществляться и ее настройка. Точки доступа могут работать как в одном (2,4 или 5 ГГц), так и в обоих диапазонах частот (*dual-mode*). При этом работа в разных частотных диапазонах может осуществляться параллельно (*concurrent dual-mode*), если такая функциональность поддерживается точкой доступа.

В зависимости от типа архитектуры беспроводной сети точки доступа можно разделить на два класса: автономные и унифицированные.

Автономные точки доступа (Autonomous Access Point) — это традиционные устройства, которые используются в домашних сетях, сетях небольших офисов, учебных классов, кафе, ресторанов, т. е. там, где не требуется большой зоны покрытия. Автономные точки доступа самостоятельно **реализуют**



DAP-1360



DAP-2695



DAP-1420



DAP-3690

Рис. 1.5. Точки доступа D-Link

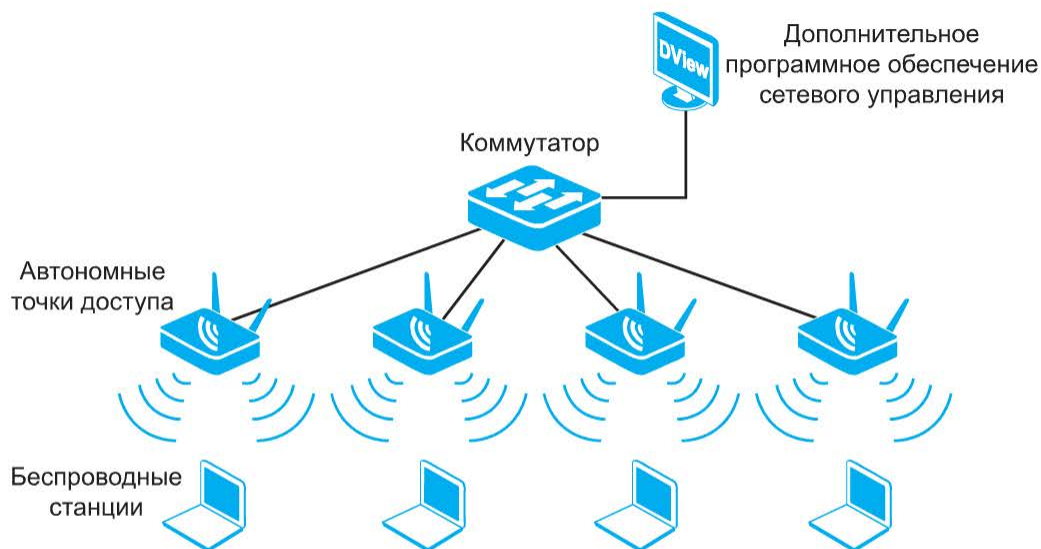


Рис. 1.6. Беспроводная сеть с автономными точками доступа

все сервисы 802.11 и поэтому работают в сети независимо друг от друга, даже если соединены через коммутаторы (рис. 1.6). В качестве примера можно привести следующие автономные точки доступа D-Link: DAP-1360U, DAP-2310, DAP-2360, DAP-2330. Настройка автономных точек доступа может выполняться как индивидуально через Web-интерфейс, так и централизованно с помощью функции AP Array или программного обеспечения сетевого управления Central WiFiManager.

Унифицированные точки доступа (*Unified Access Point*) могут работать как автономно друг от друга, реализуя все сервисы 802.11 самостоятельно, так и **централизованно контролироваться беспроводным контроллером** (рис. 1.7). В последнем случае сервисы 802.11 распределены между точками доступа и контроллерами.

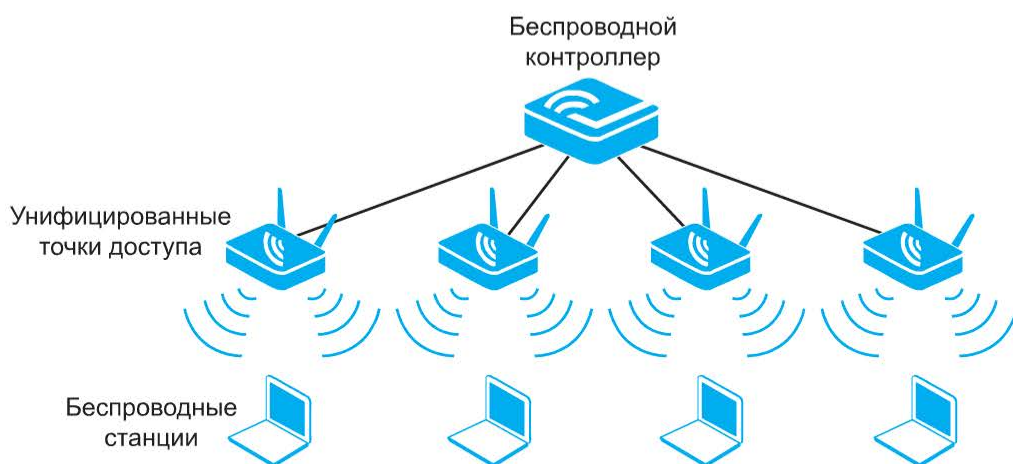


Рис. 1.7. Беспроводная сеть с централизованным управлением

Беспроводной контроллер (Wireless Controller) представляет собой устройство, основной функцией которого является управление, контроль и настройка точек доступа, присутствующих в сети (рис. 1.8). Точки доступа подключаются к контроллеру через порты Ethernet. Беспроводной интерфейс у контроллера отсутствует. В качестве примера унифицированных точек доступа можно привести следующие устройства D-Link: DWL-2600AP, DWL-3600AP, DWL-6600AP, DWL-8600AP, DWL-8610AP.



Рис. 1.8. Беспроводной контроллер D-Link DWC-2000

Беспроводные контроллеры поддерживают такие функции, как роуминг, управление доступом, шифрование данных, мониторинг клиентов и точек доступа, управление радиочастотными характеристиками. Администратор может централизованно задавать одну конфигурацию сразу для всех подключенных к контроллеру точек доступа вместо того, чтобы настраивать каждую в отдельности.

Централизованное управление упрощает добавление в беспроводную сеть новых точек доступа (например, для увеличения зоны покрытия), а также позволяет автоматически изменять конфигурацию устройств для улучшения параметров сети, например, при возникновении интерференции сигналов. Для повышения надежности сети можно выполнять резервирование беспроводных контроллеров: при выходе одного из контроллеров из строя, управление будет передано резервному.

Унифицированные точки доступа предназначены для использования в сетях средних и крупных предприятий, кампусных сетях, складских помещениях, больницах, гостиницах и т. д., где требуется обеспечить большую зону покрытия беспроводной сети. Предприятие может начать построение беспроводной сети с одной унифицированной точки доступа, работающей автономно, и постепенно, по мере расширения зоны покрытия и увеличения количества точек доступа, перейти к централизованной архитектуре.

По типу исполнения корпуса точки доступа можно разделить на внутренние (*indoor*) и внешние (*outdoor*). Внутренние точки доступа предназначены для установки внутри отапливаемых помещений, имеют пластиковый корпус и диапазон рабочих температур от 0 до 40 °С. Внешние точки доступа помещаются в металлические корпуса, обладающие защитой от проникновения твердых предметов и воды, и предназначены для установки на улице или в неотапливаемых помещениях. Корпус внешней точки доступа может быть снабжен нагревателем и вентилятором. Диапазон рабочих температур внешних точек доступа от –40 до 70 °С.

1.2.3. Беспроводные маршрутизаторы

Маршрутизаторы работают на сетевом уровне модели OSI, анализируют сетевые адреса (чаще всего IP-адреса) и определяют наилучшие маршруты передачи пакетов от источников к получателям. Маршрутизаторы могут соединять между собой как минимум две сети.

Маршрутизаторы D-Link в зависимости от модели могут иметь от 1 до 8 LAN-интерфейсов, которые используются для подключения локальных сетей, и 1–2 WAN-интерфейса, предназначенных для соединения локальных сетей с внешними сетями, как правило, с сетями интернет-провайдеров.

Беспроводные маршрутизаторы, помимо своей стандартной функциональности, имеют еще возможности точки доступа. Типовой беспроводной маршрутизатор D-Link обычно включает четырехпортовый коммутатор, точку доступа 802.11, порт WAN и порт USB, к которому может быть подключен, например, принтер или USB-модем (рис. 1.9).



DIR-615A



DIR-890L



DIR-825



DIR-880L

Рис. 1.9. Беспроводные маршрутизаторы D-Link

Точки доступа и беспроводные маршрутизаторы имеют следующие отличия:

- точки доступа соединяют клиентов только в пределах одной сети, в то время как беспроводные маршрутизаторы обеспечивают подключение к разным сетям. Принятие решения о передаче пакета основывается маршрутизатором на анализе IP-адресов, в то время как точка доступа в процессе своей работы не принимает во внимание IP-адреса отправителей и получателей (анализирует MAC-адреса);



Рис. 1.10. Пример использования в сети беспроводного маршрутизатора

• маршрутизаторы могут использовать функцию трансляции адресов (*Network Address Translation, NAT*), благодаря чему множество устройств сети совместно используют один IP-адрес, выделенный провайдером услуг для подключения к Интернету. Также маршрутизаторы могут поддерживать функции межсетевого экрана и динамически присваивать клиентам IP-адреса и сведения об IP-конфигурации с помощью протокола DHCP (*Dynamic Host Configuration Protocol*) (рис. 1.10). Другими словами, беспроводные маршрутизаторы обладают более развитым функционалом по сравнению с точками доступа.

Применение беспроводных маршрутизаторов наиболее удобно в домашних сетях и сетях небольших офисов. Они позволяют подключать к Интернету как проводных, так и беспроводных клиентов, поддерживают функции безопасности, а также динамической конфигурации IP-адресов клиентов. В больших сетях установка беспроводных маршрутизаторов нецелесообразна, поскольку в таких структурах обычно имеются выделенные серверы DHCP, межсетевые экраны, а централизованное управление точками доступа значительно проще, чем маршрутизаторами.

1.2.4. Беспроводные повторители

Беспроводные повторители восстанавливают (усиливают) радиосигналы с целью увеличения радиуса действия беспроводной сети. Повторитель физически не соединяется ни с одной частью беспроводной сети. Вместо этого он получает сигналы от точки доступа, клиентского устройства, беспроводного маршрутизатора или другого повторителя в определенном радиочастотном канале, усиливает и ретранслирует их в том же самом канале, не изменяя передаваемый кадр (рис. 1.11).

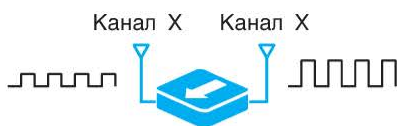


Рис. 1.11. Принцип работы беспроводного повторителя

Повторитель располагается между точкой доступа и удаленным устройством и действует как ретранслятор кадров, передаваемых между ними. Таким образом он позволяет бороться с затуханием радиочастотных сигналов и позволяет увеличивать зону покрытия. Например, провайдеры услуг зачастую устанавливают беспроводные маршрутизаторы у входа в квартиру. Ввиду особенностей планировки зона покрытия может не охватывать все комнаты. Одним из способов увеличения зоны покрытия в квартире является использование беспроводных повторителей (рис. 1.12).

В качестве повторителя используется либо точка доступа, настроенная на работу в режиме повторителя, либо специализированное устройство — автономный повторитель (рис. 1.13).

Несмотря на расширение зоны покрытия, использование беспроводных повторителей в сети приводит к снижению ее пропускной способности. По-



Рис. 1.12. Пример использования беспроводного повторителя



Рис. 1.13. Беспроводные повторители D-Link

вторители принимают и передают один и тот же кадр, что приводит к удвоению числа кадров, передаваемых в беспроводной сети. При планировании беспроводной сети не рекомендуется использовать в ней больше трех повторителей.

1.2.5. Беспроводные мосты

Проводные сети, находящиеся как на небольшом расстоянии друг от друга — в соседних зданиях или комнатах внутри одного здания, так и на значительных расстояниях (до нескольких километров), объединяют с помощью *беспроводных мостов* (рис. 1.14). При соединении сетей, находящихся на больших расстояниях друг от друга, к мостам, как правило, подключаются направленные антенны.



Рис. 1.14. Беспроводной мост D-Link DAP-1513

Мосты, предназначенные для использования внутри помещений, позволяют подключить к беспроводной сети от одного до нескольких устройств, не имеющих беспроводного интерфейса. Например, их удобно использовать при подключении таких устройств, как принтеры или игровые консоли, имеющие только порт Ethernet (рис. 1.15).

Мост пересылает через себя кадры только в том случае, если физический адрес (MAC-адрес) узла назначения принадлежит другому сегменту сети или другой сети.

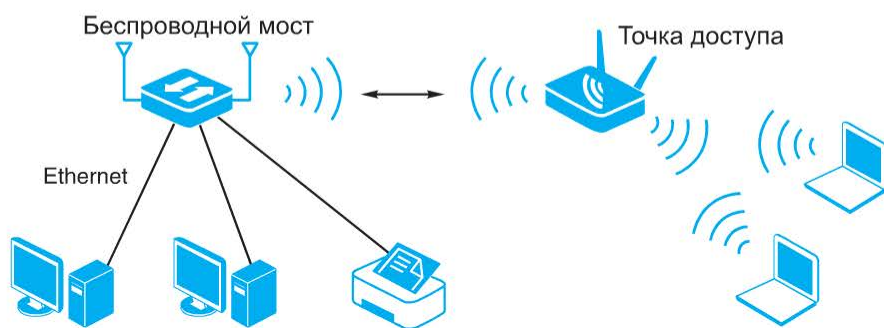


Рис. 1.15. Сеть с применением беспроводного моста

В качестве беспроводных мостов могут использоваться точки доступа, настроенные для работы в режиме моста, например DAP-1533, DAP-3760, DAP-3860. Также компания D-Link производит автономные беспроводные мосты, например DAP-1513.

1.2.6. Антенны

В отличие от проводных сетей, где сигналы передаются по кабельной проводке, например медным витым парам или оптическим волокнам, в беспроводных сетях физической средой передачи является атмосфера и открытый космос. В кабельных средах передача всегда направленная (осуществляется между точками подключения кабеля), а беспроводные физические среды не могут направлять сигналы только в определенном направлении. Для построения беспроводных линий связи каждый узел оснащается *антенной*. Антенну можно определить как проводник (или систему проводников), используемый для излучения и приема электромагнитных волн из окружающего пространства. Для передачи радиочастотного сигнала электрические импульсы передатчика, несущие информацию пользователя, с помощью передающей антенны преобразуются в электромагнитную энергию, которая излучается в окружающее пространство (атмосферу, космос, воду). При получении сигнала энергия электромагнитных волн, поступающих на приемную

антенну, преобразуется в электрические импульсы, после чего попадает на приемник для дальнейшего извлечения из сигнала полезной информации.

Основные характеристики антенн

Как правило, при двухсторонней связи одна и та же антенна может быть использована как для приема, так и для передачи сигналов. Это связано с тем, что характеристики антенны одинаковы для процессов получения и передачи электромагнитной энергии.

Основной характеристикой антенны является **направленность**, отражающая зависимость напряженности (мощности) электромагнитного поля, излучаемого или принимаемого антенной, от угловых координат. По виду характеристики направленности антенны можно разделить на *всенаправленные* (*omni-directional*) и *направленные* (*directional*). Всенаправленные антенны также называются *ненаправленными*, поскольку они не имеют четко выраженного направления распространения излучения радиоволн.

При ненаправленной передаче (с использованием всенаправленной антенны) передаваемый сигнал распространяется во всех направлениях и может быть принят множеством антенн. При направленной передаче передающая антенна излучает сфокусированный электромагнитный луч, поэтому передающая и приемная антенны должны быть тщательно нацелены (рис. 1.16).

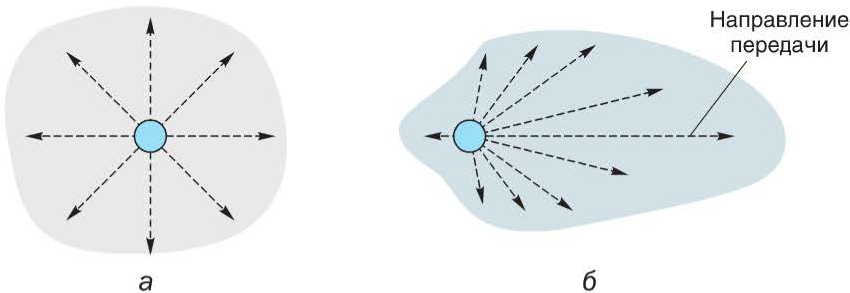


Рис. 1.16. Излучение всенаправленной (а) и направленной (б) антенны

Коэффициент усиления (*antenna gain*) G является мерой *направленности* антенны и определяется как отношение мощности сигнала P_1 , излученного в направлении передачи, к мощности сигнала P_2 , излучаемого идеальной (изотропной) антенной в любом направлении:

$$G = \frac{P_1}{P_2},$$

т. е. является безразмерной величиной. На практике он выражается через логарифмическое отношение мощностей, напряжений или токов и измеряется в децибелах (dB, дБ):

$$G = 10 \lg \frac{P_1}{P_2}.$$

В технических описаниях антенн единицы измерения коэффициента усиления выражаются в изотропных децибелах — dBi (дБи) (дополнительный индекс «i» («и») обозначает *isotropic* — изотропный), таким образом уточняется, что мощность излучения антенны в определенном направлении сравнивается с мощностью излучения изотропной антенны.

Изотропная антенна — это идеальная (в теоретическом отношении) антенна, излучающая электромагнитную энергию с одинаковой интенсивностью во всех направлениях (рис. 1.17).

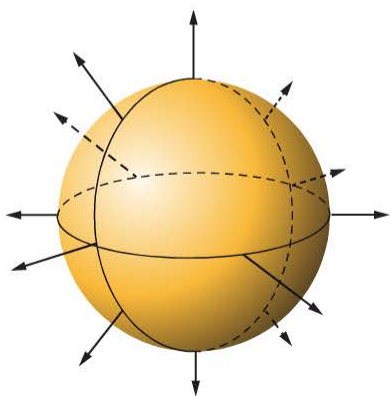


Рис. 1.17. Изотропная антенна

Использование термина «коэффициент усиления» зачастую приводит к ошибочному предположению, что антенны способны усиливать сигнал. На самом деле это неверно: антенны представляют собой пассивные устройства, не имеющие источников энергии для усиления передаваемого сигнала. Коэффициент усиления антенны показывает *фокусировку мощности* в определенном направлении, а не *усиление* ее. Например, если коэффициент усиления антенны в заданном направлении составляет 5 dBi, это означает, что в данном направлении мощность излучения на 5 дБ (в 3,16 раза) больше, чем мощность излучения идеальной изотропной ан-

тенны при одинаковой мощности передатчика. При этом увеличение мощности сигнала в одном направлении происходит за счет уменьшения мощности излучения в остальных направлениях распространения радиоволн.

Для того чтобы лучше понять принцип фокусировки энергии в разных направлениях, представьте изотропную антенну, показанную на рис. 1.17, в виде резинового мяча. Представьте, что на мяч сильно надавили сверху (в вертикальном направлении), он немного растянулся, но сохранил форму круга в горизонтальной плоскости, а в вертикальной сжался под действием силы, приняв форму эллипса. Этот пример можно использовать для описания принципа действия направленной антенны, которая фокусирует большее количество энергии в горизонтальной плоскости за счет уменьшения излучения энергии в вертикальной. В горизонтальной плоскости такая антенна по-прежнему остается всенаправленной. Прикладывая к резиновому мячу различные усилия, можно менять его форму, добившись, например, конусообразной. Таким образом можно представить себе принцип излучения направленной антенны.

Графическим представлением зависимости коэффициента усиления (или характеристики направленности) от направления антенны в заданной плоскости является **диаграмма направленности (ДН)**, показанная на рис. 1.18. Как правило, диаграммы направленности антенн представляются как два поперечных сечения трехмерной диаграммы — горизонтальное и вертикальное. В этом случае диаграмма направленности представляет собой замкнутую

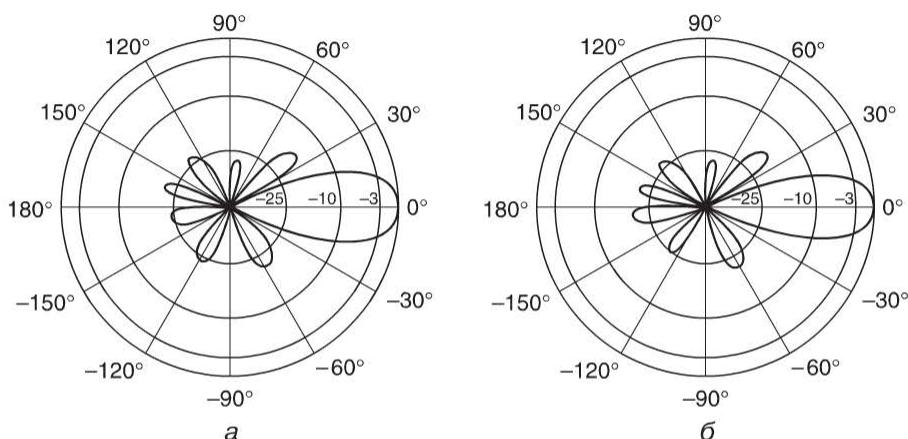


Рис. 1.18. Диаграммы направленности направленной антенны в горизонтальной (а) и вертикальной (б) плоскостях

линию в полярной системе координат, построенную таким образом, чтобы расстояние от антенны (центр диаграммы) до любой точки диаграммы направленности было бы прямо пропорционально энергии, излучаемой антенной в данном направлении.

Направление излучения максимальной мощности называется главным (основным) лепестком антенны. Остальные лепестки диаграммы направленности антенны называются боковыми, а лепесток излучения в сторону, обратную главному направлению, называется задним лепестком диаграммы направленности антенны (рис. 1.19).

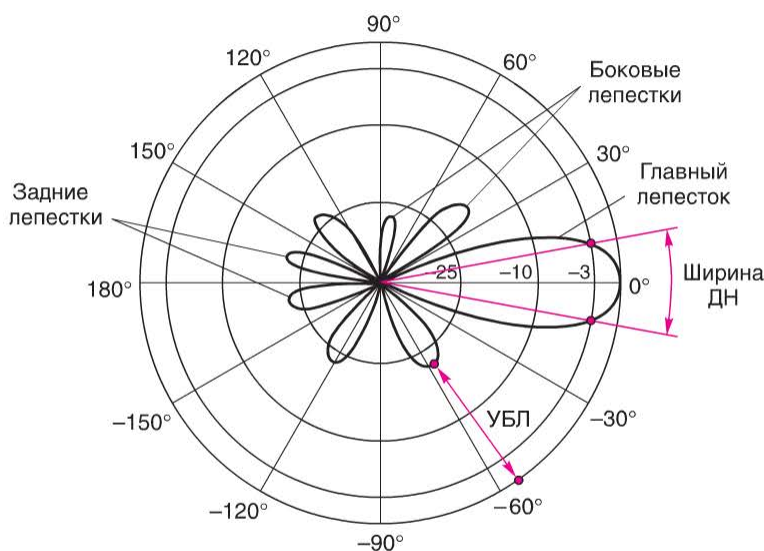


Рис. 1.19. Параметры антенны на диаграмме направленности

Важным параметром антенны является **ширина диаграммы направленности** (ширина основного лепестка), под которой понимают угол между двумя направлениями, вдоль которых напряженность поля (или плотность потока мощности) падает до определенного значения. Ширина ДН измеряется в градусах. На практике обычно оценивают ширину ДН при уменьшении напряженности поля на 3 дБ (в 2 раза) — $\Delta\theta_{-3}$. В этом диапазоне углов снижением мощности передаваемого сигнала при построении беспроводной линии связи можно пренебречь.

Зачастую ширину ДН оценивают по нулевому уровню $\Delta\theta_0$, т. е. когда напряженность поля главного лепестка падает с максимального значения до нуля. Данная величина показывает диапазон углов, где излучается вся энергия главного лепестка ДН, и используется при создании систем компенсации радиопомех, в которых в приемник поступает только информация, полученная по главному лепестку ДН, а помехи, принимаемые по боковым лепесткам ДН, устраняются. Другими словами, при построении линии связи с направленной антенной приемник беспроводного сигнала должен находиться в зоне ее главного лепестка, в противном случае передача информации будет неустойчивой и/или невозможной.

Еще одной характеристикой антенны является **уровень боковых лепестков** (УБЛ), который определяется как отношение величины напряженности поля в направлении максимума бокового лепестка наибольшего уровня к величине напряженности поля в направлении максимума главного лепестка. Величина УБЛ, как правило, выражается в децибелах и определяет степень побочного излучения антенной электромагнитного поля, что влияет на качество электромагнитной совместимости с расположенными неподалеку радиоэлектронными системами. Поэтому при создании антенны стремятся к максимальному снижению уровня боковых лепестков.

При подключении к антенне передатчика его энергия должна приниматься антенной и передаваться дальше в окружающее пространство. Часть этой энергии теряется, рассеиваясь в антенне — тратится на нагрев. Отношение полезной мощности излучения ко всей мощности, получаемой антенной, называется **коэффициентом полезного действия** (КПД) антенны. Для простых металлических антенн он обычно равен 95–99 %, т. е. большая часть энергии сигнала преобразуется антенной в электромагнитное поле и излучается в свободное пространство.

В общем случае мощность, излучаемая антенной, делится на полезную (активную) и реактивную. Активная мощность, называемая еще мощностью излучения, формирует электромагнитную волну, переносящую передаваемый сигнал от передающей антенны к приемной. Реактивная мощность характеризует колеблющееся вокруг антенны реактивное поле, не участвующее в передаче сигнала приемнику. Если вблизи антенны будут находиться посторонние предметы, то под действием реактивного поля в них будет возникать электрический ток, на формирование и поддержание которого будет расходоваться полезная энергия. Это приводит к снижению мощности излучения и увеличению мощности потерь. Таким образом, для антенны можно ввести

понятие **сопротивления**, измеряемого в омах (Ом) и отражающего степень потерь полезной энергии на нагрев проводников и изоляции антенны, а также наведение токов с тепловыми потерями на предметах вблизи антенны. Другими словами, сопротивление антенны показывает ее способность препятствовать преобразованию всей энергии в энергию излучения.

Мощность излучения антенны определяется как квадрат тока на входе антенны, умноженный на ее активное сопротивление. Реактивная мощность характеризуется реактивным сопротивлением. Таким образом, получается, что каждая антенна имеет свое *комплексное входное сопротивление Z* :

$$Z = R + jX,$$

где R — активное сопротивление антенны; X — реактивное сопротивление антенны; $j = \sqrt{-1}$ — мнимое число. В идеале при создании и размещении антенны необходимо стремиться к максимальному уменьшению реактивной составляющей входного сопротивления антенны.

Входное сопротивление антенны зависит от геометрической формы и размеров, а также материала антенны. Согласно теореме взаимности, значения входного сопротивления антенны в режимах передачи и приема совпадают. Кроме того, сопротивление антенны зависит от частоты передаваемого сигнала. Изменение сопротивления от частоты показывает **диапазон частот (диапазонность)** антенны, в котором она может эффективно работать. Диапазон частот выражается в мегагерцах (МГц, MHz) или гигагерцах (ГГц, GHz).

Из теории электрических цепей известно, что максимальная мощность передается от генератора в нагрузку тогда, когда *сопротивления генератора и нагрузки согласованы*. Под согласованием понимается устранение (компенсация) реактивной составляющей сопротивления и равенство активного сопротивления линии передачи активному сопротивлению нагрузки (в нашем случае антенны). При таком согласовании потери энергии при передаче будут малы и ограничатся только потерями в металлическом проводнике и диэлектрике коаксиального кабеля, соединяющего генератор и нагрузку (антенну). Другими словами, согласование сопротивления оконечного каскада передатчика (или входного каскада приемника) и сопротивления антенны является условием передачи максимальной мощности.

При наличии такого согласования мощность от передатчика полностью передается в антенну в режиме так называемой бегущей волны (волны, переносящей энергию от передатчика к антенне). Если согласования добиться не удастся, то между антенной и передатчиком (или приемником) возникнет отраженная волна (стоячая волна), и часть мощности будет возвращаться от антенны назад в передатчик (или от приемника к антенне). Чем хуже согласование, тем больше отраженная стоячая волна. Поэтому для характеристики *качества согласования* используют **коэффициент стоячей волны (КСВ, англ. Standing Wave Ratio, SWR)**, который определяется как отношение наибольшего значения амплитуды напряженности электрического или магнитного

поля стоячей волны в линии передачи к наименьшему. Другими словами, это отношение наибольшей амплитуды отраженной волны к наименьшей.

Желательно, чтобы значение КСВ в линии передачи было близко к единице, при этом максимален КПД системы «линия передачи — антенна», равный отношению мощности, выделяемой в нагрузку, к мощности падающей волны, отдаваемой генератором в линию передачи. Допустимые значения КСВ на рабочей частоте или в полосе рабочих частот для различных устройств регламентируются в технических условиях, спецификациях и ГОСТах.

В коаксиальном кабеле КСВ можно определить по напряжению как отношение наибольшего вдоль линии значения амплитуды напряжения к наименьшему. В этом случае говорят о КСВ **по напряжению** (КСВН, англ. *voltage, VSWR*). Обычно приемлемые для антенны значения КСВ (или КСВН) находятся в пределах от 1,1 до 2,0.

Для удобства согласования множества антенн с беспроводными устройствами производители используют *универсальное сопротивление величиной 50 Ом*. Такое сопротивление имеют радиопорты всех беспроводных устройств и антенн стандарта 802.11, что позволяет подключать различные антенны к устройствам без потери эффективности их работы.

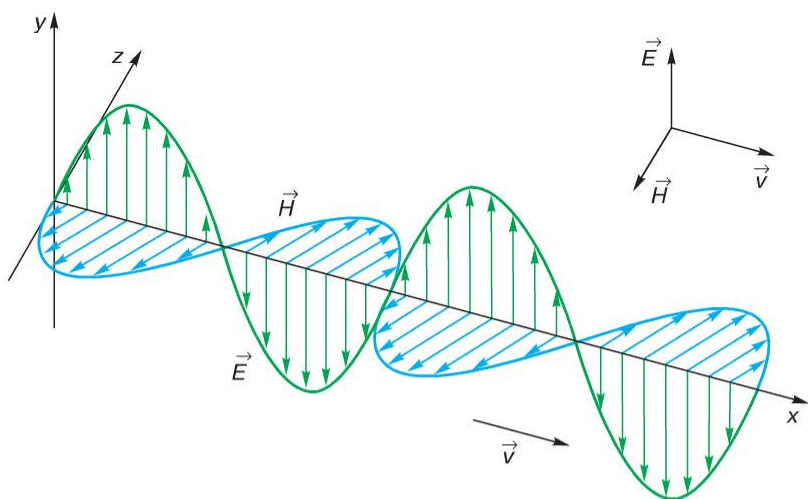


Рис. 1.20. Поляризация электромагнитной волны

Еще одной важной характеристикой антенны является способность излучать и взаимодействовать при приеме с электромагнитным полем определенной **поляризации**. Под поляризацией волн понимается характеристика, описывающая поведение вектора колеблющейся величины в плоскости, перпендикулярной направлению распространения волны. Поляризацию электромагнитных волн оценивают по поведению вектора электрической напряженности \vec{E} электромагнитного поля в плоскости, перпендикулярной

направлению распространения волны. Если расположить тонкую проволочную антенну вдоль оси y (рис. 1.20), то при протекании по ней электрического тока некоторой частоты она будет излучать поле в направлении волнового вектора \vec{v} .

Колеблющиеся векторы напряженности электрического \vec{E} и магнитного \vec{H} полей перпендикулярны направлению распространения волны. Поляризация волны определяется через проекцию вектора \vec{E} на плоскость xz . Если проекция является линией, то говорят о *линейной* поляризации, если окружностью или эллипсом — о *круговой* или *эллиптической*. Линейная поляризация может быть вертикальной и горизонтальной (относительно поверхности Земли). Круговая (эллиптическая) поляризация может быть правого или левого вращения (рис. 1.21).

Поляризация волн в некоторых случаях может оказывать значительное влияние на качество связи. Если при построении беспроводного моста с расстоянием между антеннами сотни метров и более одна антенна будет работать только с линейной горизонтальной поляризацией, а другая с вертикальной, то связь будет неустойчивой или отсутствовать вообще. Причина состоит в том, что поле с линейной поляризацией не влияет на поле с вертикальной поляризацией. Однако это может быть полезно для систем МИМО (англ. *Multiple Input Multiple Output* — множество входов и множество выходов) с несколькими антеннами, каждая из которых передает разные сигналы с разной поляризацией. При использовании двух антенн с разными линейными поляризациями можно создать систему с двумя независимыми каналами (не создающими друг другу радиопомех), увеличив тем самым скорость передачи в 2 раза.

При создании беспроводных мостов без использования системы МИМО необходимо использовать антенны с одинаковой поляризацией и ориентировать их по поляризации (*согласовать антенны по поляризации*).

Однако при работе внутри помещений из-за наличия многократных переотражений от окружающих предметов — мебели, стен здания и в особенности металлических, поляризация волн меняется (линейная горизонтальная может измениться на вертикальную). Поэтому внутри помещений согласовывать антенны по поляризации необязательно.

Использование круговой поляризации эффективно при связи с движущимися объектами (например, с вращающимся снарядом или ракетой) и малоприспособно для систем стандарта 802.11 малого радиуса действия. К тому же конструкции таких антенн сложнее, что приводит к удорожанию антенных систем.

Классификация антенн

К антеннам беспроводных устройств стандарта 802.11 предъявляются различные, иногда противоречивые, требования по весу, размерам, стоимости, эргономичности, универсальности использования. В настоящее время существует большое число различных конструкций антенн, каждая из которых

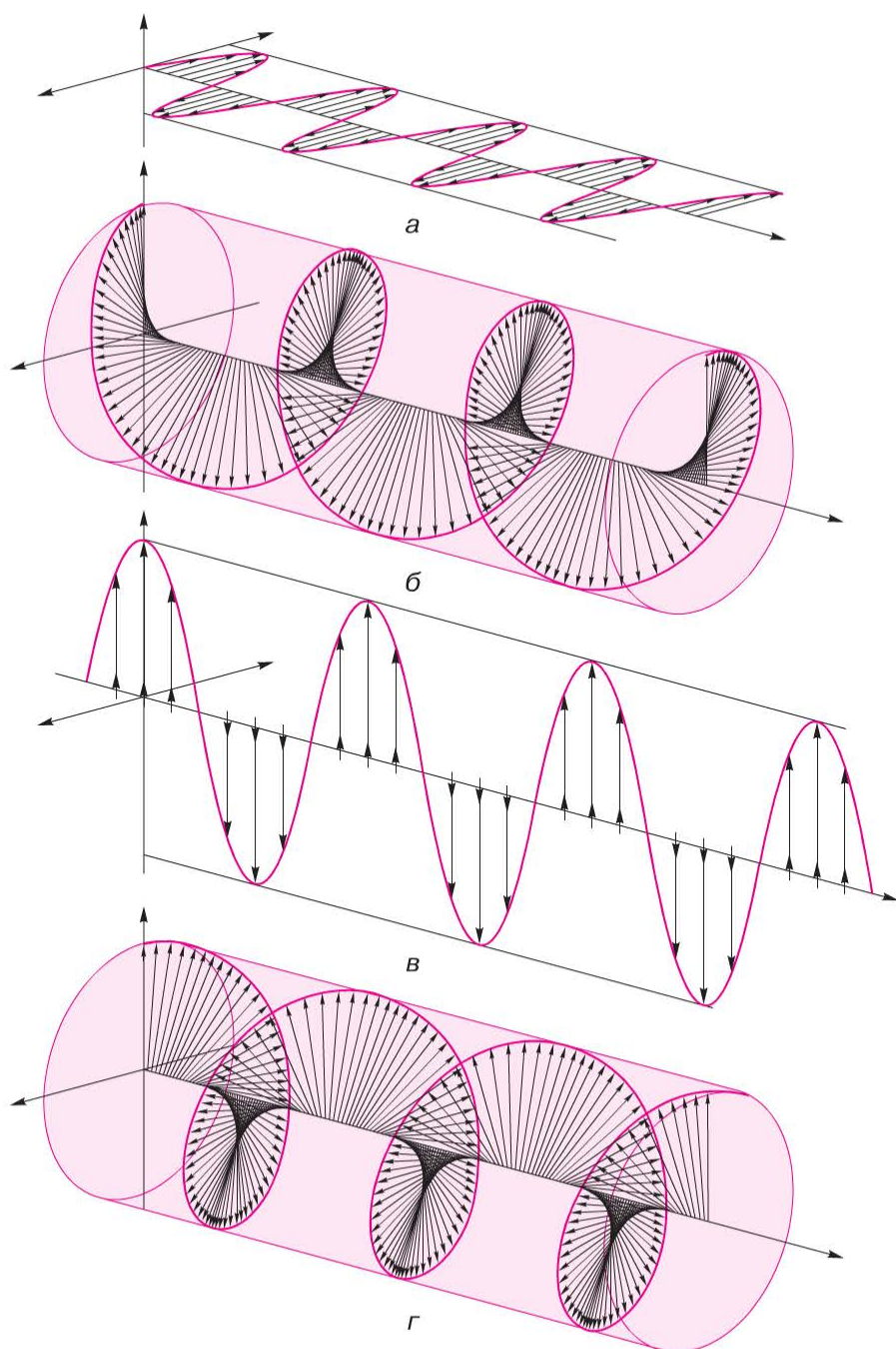


Рис. 1.21. Разновидности поляризации волн:

а — горизонтальная линейная поляризация; *б* — круговая поляризация левостороннего вращения; *в* — вертикальная линейная поляризация; *г* — круговая поляризация правостороннего вращения

имеет свои достоинства и недостатки и потому по-разному удовлетворяет предъявляемым требованиям (рис. 1.22).

Классификация антенн может быть проведена по разным признакам: направленности, поляризации, взаимодействию с электромагнитным полем, конструктивным типам, диапазону частот, назначению и исполнению.

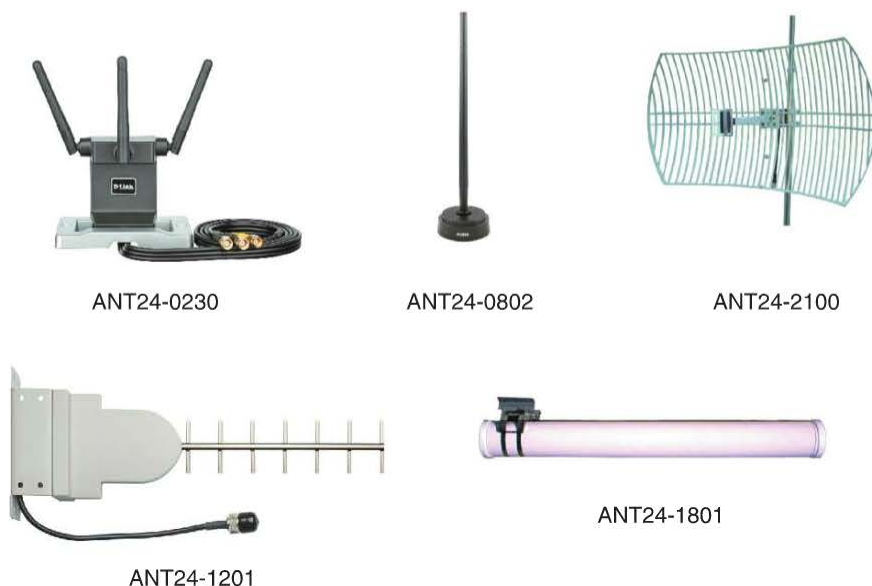


Рис. 1.22. Типы исполнения антенн D-Link

По *направленности* антенны разделяют на *всенаправленные* и *направленные*. Поскольку пользователи беспроводных сетей обычно располагаются вокруг точек доступа, то самым распространенным типом антенн являются всенаправленные антенны. Поэтому большинство производимых точек доступа оснащено всенаправленными антеннами с небольшим коэффициентом усиления из-за отсутствия направленности (обычно от 2 до 5 dBi). Такой тип антенн наиболее подходит для создания беспроводных сетей внутри зданий. Всенаправленные антенны обеспечивают широкую зону покрытия и при настройке точек доступа на работу в неперекрывающихся по частоте каналах позволяют создавать перекрытие зон их покрытия. Это дает пользователям возможность не терять подключение к беспроводной сети при перемещении по зданию или большому офису (рис. 1.23).

При проектировании беспроводных сетей важно понимать, что фактическое распространение электромагнитных волн может отличаться от диаграммы направленности антенны, которая основана на распространении сигналов в зоне прямой видимости. В большинстве случаев между передат-

чиком и приемником встречаются различного рода препятствия. В помещениях такими препятствиями служат стены, потолки, мебель, на открытом пространстве — дома, деревья, транспорт. При встрече на пути своего распространения препятствий электромагнитные волны могут отражаться от них, преломляться, рассеиваться или огибать препятствия. Наличие препятствий между передатчиком и приемником беспроводного сигнала в большинстве случаев приводит к увеличению длины пути, проходимого сигналом, вследствие чего уменьшает его мощность на входе приемника и скорость передачи информации.

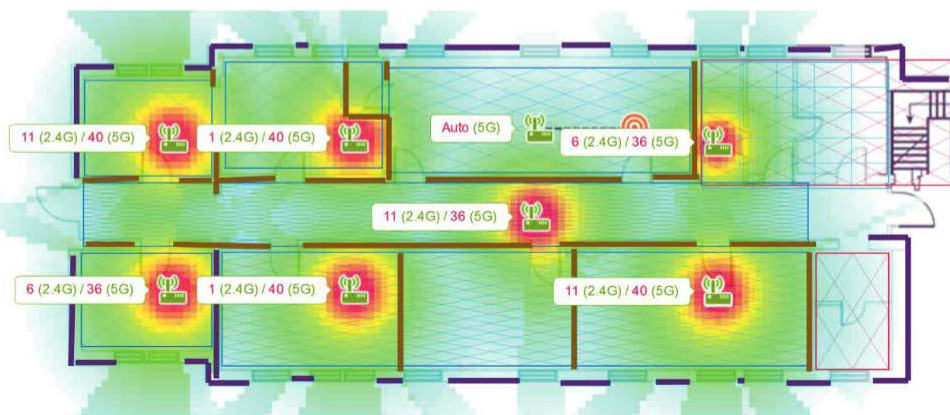


Рис. 1.23. Покрытие помещения беспроводной сетью с точками доступа, оснащенными всенаправленными антеннами

Направленные антенны наилучшим образом подходят для организации соединений типа «точка-точка» (беспроводных мостов) между зданиями или для обеспечения зоны покрытия протяженных, но узких областей. Например, такие антенны удобно использовать при передаче сигналов между отдельными зданиями, внутри которых уже используются всенаправленные антенны.

По *поляризации* антенны классифицируются на антенны *вертикальной, горизонтальной и круговой поляризации*. Та или иная поляризация может быть получена на антенне любого типа. Выбор типа антенны для создания определенной поляризации определяется размерами, простотой изготовления и конечной стоимостью антенны.

По *взаимодействию с электромагнитным полем* антенны можно разделить на *электрические* и *магнитные*. Электрическая антенна реагирует на электрическую составляющую электромагнитных волн, а магнитная — на магнитную составляющую. Простейшим примером электрической антенны является отрезок металлической проволоки (проволочная антенна), к середине которого подключен передатчик (генератор радиоволн). В теории антенн такая антенна называется симметричным электрическим вибратором. Электрический ток подается с генератора на оба конца антенны и, протекая по поверхности, приводит к появлению на них разности потенциалов (электрического

напряжения), которое создает вокруг антенны электрическое поле. Поскольку ток переменный, то электрическое поле и порожденное им магнитное поле также переменные. Таким образом возникает электромагнитная волна, переносящая получаемый полезный сигнал в пространстве конечным потребителям. Достоинствами таких антенн является простота конструкции, относительно невысокая стоимость, высокий коэффициент полезного действия. Электрические антенны широко применяются в различных системах передачи информации по всему миру, в том числе и в системах стандарта 802.11. На практике для удобства слово «электрическая» опускают.

Примером магнитной антенны является магнитная рамка, иногда используемая в помещениях в качестве приемной телевизионной антенны. При ее подключении к генератору ток, текущий по кругу антенны, не приводит к появлению электрической разности потенциалов, а следовательно, и не формирует электрическое поле. Однако ток, текущий по окружности, создает магнитное поле, перпендикулярное плоскости этой окружности. Если ток переменный, то возникает переменное магнитное поле, которое, в свою очередь, создает переменное электрическое поле, что приводит к формированию электромагнитной волны. Достоинствами такой антенны являются простота конструкции и улучшенный прием в помещениях (поскольку магнитная составляющая электромагнитного поля лучше проникает в помещения). Недостатком антенны является очень низкий коэффициент полезного действия, что делает ее малоэффективной при передаче сигналов. Кроме того, такая антенна может эффективно работать лишь в узкой полосе частот. Отмеченные недостатки привели к тому, что магнитные антенны не используются в беспроводных сетях стандарта 802.11.

По конструктивным типам антенны классифицируются на *линейные* и *апертурные*. *Линейными* антеннами называются любые излучающие системы малого (по сравнению с длиной) поперечного размера и с переменными токами, текущими вдоль оси системы. К линейным относятся проволочные антенны и их комбинации, а также щелевые, полосковые и микрополосковые антенны. Проволочные антенны (называемые также *штыревыми*) обычно выполняются из тонкого металлического цилиндра (проволоки) или полый трубки, иногда покрытой диэлектриком (например, антенна ANT24-0802, показанная на рис. 1.22). Диаграммы направленности такой антенны представлены на рис. 1.24.

Антенна ANT24-0230 (см. рис. 1.22) состоит из трех проволочных антенн, каждая из которых имеет свой независимый вход.

К линейным антеннам также относят антенны бегущей волны, распространяющейся вдоль оси антенны по направлению излучения активного (питаемого от генератора) элемента и наводящей токи в элементах антенны, что способствует повышению коэффициента усиления благодаря сложению волн, излучаемых впоследствии каждым элементом. Одной из таких антенн является антенна типа волновой канал, известная так же как антенна Яги-Уда или антенна Яги (*Yagi antenna*). Она состоит из расположенных вдоль линии

излучения параллельно друг другу активного и нескольких пассивных вибраторов (называемых также директорами). Такую антенну также называют директорной. К антеннам Яги относятся антенны ANT24-1201 и ANT24-1801 (см. рис. 1.22).

На рис. 1.25 показано внутреннее устройство антенны ANT24-1201. Активный элемент и рефлектор выполнены по технологии изготовления печатных плат, а директоры — в виде проволочной конструкции, позволяющей увеличить коэффициент усиления до 12 дБи.

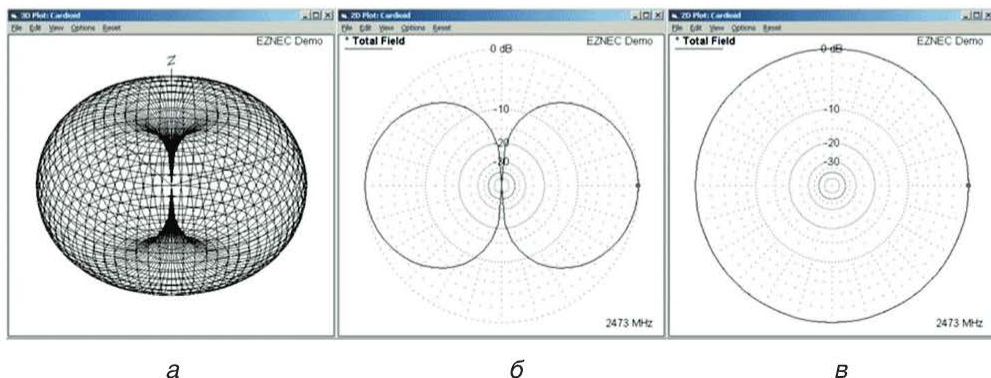


Рис. 1.24. Диаграммы направленности штыревой антенны:
а — трехмерная; б — в вертикальной и в — в горизонтальной плоскости

На рис. 1.26 показано внутреннее устройство антенны ANT24-1801, представляющей собой директорную антенну на металлической траверсе, соединяющей между собой элементы антенны. Для защиты от погодных условий такая антенна закрыта пластиковым цилиндрическим кожухом. Наличие большого числа элементов приводит к тому, что ширина ДН сужается до 15° , что приводит к возрастанию коэффициента усиления до 18 дБи.



Рис. 1.25. Внутреннее устройство антенны ANT24-1201

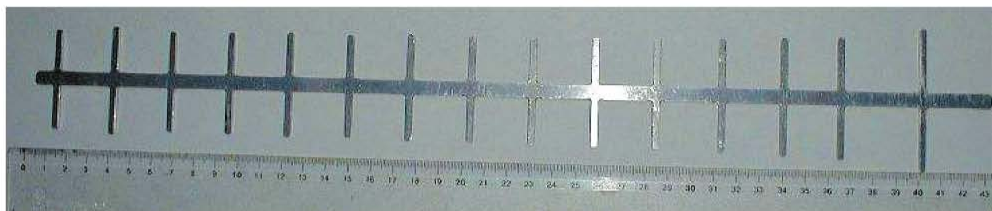


Рис. 1.26. Внутреннее устройство антенны ANT24-1801

Характерной особенностью линейных антенн является слабая зависимость распределения тока вдоль их оси от конфигурации провода. Поэтому к линейным антеннам относятся не только прямолинейные антенны, но и искривленные, изогнутые и свернутые провода (например, свернутые в спираль — спиральная антенна), щели и полоски, если их поперечные размеры много меньше продольных и меньше длины волны.

Полосковая или патч-антенна (от англ. *patch*) является важным типом линейных антенн, используемым в сетях 802.11. Полосковая антенна состоит из металлической пластины, являющейся излучателем и расположенной на малом (относительно длины радиоволны) расстоянии от плоского металлического экрана. Зазор между излучателем и экраном может быть заполнен диэлектриком (пенопласт, полиэтилен, фторопласт, полистирол). Если его диэлектрическая проницаемость близка к единице, то антенну называют полосковой, а если проницаемость больше 8 — микрополосковой. Применение микрополосковой технологии позволяет существенно снизить размеры, массу и стоимость антенны. Такая антенна может изготавливаться по той же технологии, что и печатные платы, и называться полосковой печатной антенной.

Компания D-Link выпускает по полосковой технологии антенны ANT24-0600, ANT24-0801, ANT24-1400. Внешний вид и внутренняя компоновка антенны ANT24-1400 показаны на рис. 1.27.



Рис. 1.27. Антенна ANT24-1400

На рис. 1.28 показаны встроенные антенны маршрутизатора DIR-615. Применение встроенных антенн позволяет уменьшить размеры и улучшить дизайн беспроводного устройства.

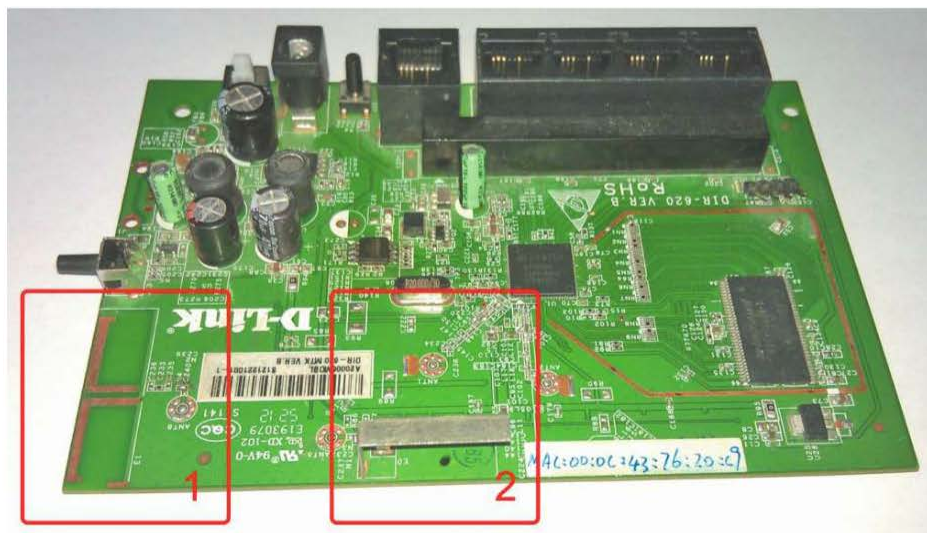


Рис. 1.28. Антенны маршрутизатора DIR-615:

1 — печатная микрополосковая; 2 — полосковая

Апертурными называются антенны, излучатель/приемник электромагнитных волн которых образован некоторой поверхностью (плоскостью), называемой апертурой. Такое название выбрано по аналогии с оптикой, в которой под апертурой понимается размер объектива, отвечающего за количество поступающего на светочувствительные элементы фотокамеры света. Классификация апертурных антенн по типам весьма обширна и включает в себя такие антенны, как волноводные, рупорные, линзовые, зеркальные, щелевые, диэлектрические, импедансные (бегущей волны). Каждому типу антенн присущи те или иные достоинства и недостатки, поэтому разные типы антенн применяются в разных диапазонах частот, а также при решении разных задач передачи сигнала на расстоянии. Рассмотрим подробнее только те типы апертурных антенн, которые используются в беспроводных устройствах стандарта 802.11.

Для увеличения коэффициента усиления антенны необходимо увеличить ее площадь (площадь излучающей/принимающей поверхности). Наиболее подходящей конструкцией для этого подхода является зеркальная антенна, состоящая из металлического отражателя (зеркала) и расположенного на некотором расстоянии от него облучателя. Основное достоинство зеркальной конструкции состоит в том, что за счет специальной формы зеркала антенна способна собирать все приходящие лучи в одной точке (фокусе), в которой

устанавливается облучатель. При излучении все лучи, исходящие от облучателя, по закону геометрической оптики преобразуются в параллельный поток лучей, повышая тем самым коэффициент усиления антенны. Облучатель представляет собой маленькую антенну какого-либо типа (проволочную, рупорную, волноводную, щелевую).

Поскольку зеркальная антенна имеет высокое усиление, она используется вне помещений в основном для создания беспроводных мостов. Основной недостаток такой конструкции в том, что она создает высокую парусность (сопротивление ветру), что может привести к поломке антенны при сильном ветре. Парусность антенны можно снизить за счет перфорирования (от лат. *perforo* — пробиваю) отверстий зеркала антенны или построения его из набора проводников (рис. 1.29).

Показанная антенна имеет низкую парусность при высоком усилении. При построении такой конструкции необходимо предотвратить прохождение волн через зеркало. Это достигается снижением размера отверстий до величины, меньшей половины длины волны рабочей частоты. Например, для частоты 2437 МГц (центральная частота 6-го канала в диапазоне 2,4 ГГц), размер отверстий должен быть не более 62 мм. При таких размерах электромагнитная волна не сможет пройти через зеркало и будет полностью отражаться от него в нужном направлении. В антенне ANT24-2100 требуемое расстояние между проводниками соблюдается в горизонтальной плоскости. Поскольку поляризация данной антенны является вертикальной, то в вертикальной плоскости расстояние между проводниками можно увеличить, так как на прохождение и отражение радиоволн они не влияют.

По *диапазонам частот* антенны разделяются на *широкополосные* и *узкополосные*. Широкополосность является важным параметром антенны и показывает диапазон частот, в котором антенна сохраняет свои основные характеристики (направленность, мощность излучения). Недостаточная широкополосность антенны приводит к тому, что ее диаграмма направленности изменяется при изменении частоты, что влечет за собой изменение коэффициента усиления при смене рабочего канала и, как следствие, уменьшение скорости передачи. В качестве примера рассмотрим изменение диаграммы направленности антенны D-Link ANT70-1800 (рис. 1.30 и 1.31).

Как видно из рис. 1.31, при изменении частоты изменяется ширина главного лепестка (и соответственно мощность излучения в главном направлении), а также уровень боковых лепестков, что приводит к повышению мощности передаваемого сигнала в ненужных направлениях, которое может создать помехи для других устройств. Такие изменения возникают потому, что сопротивление антенны не удается согласовать с сопротивлением соединительной линии в широкой полосе частот.

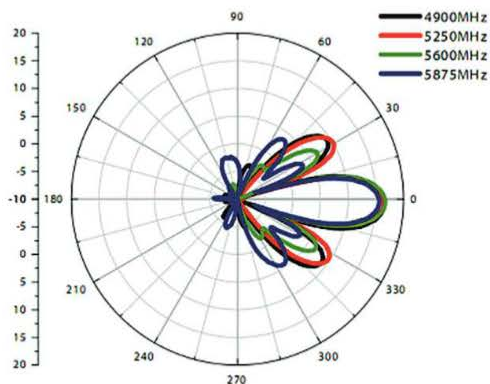
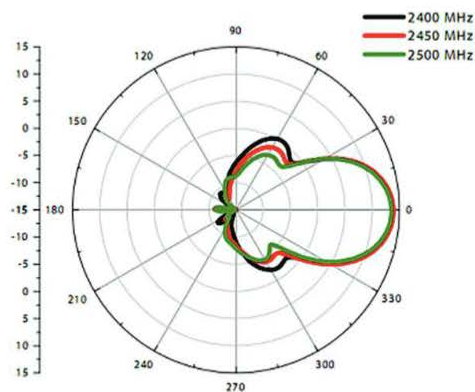
Антенна будет работать эффективно только в том случае, если диапазон ее частот будет совпадать с диапазоном частот, поддерживаемым беспроводным устройством. Поэтому по диапазонам рабочих частот антенны устройств



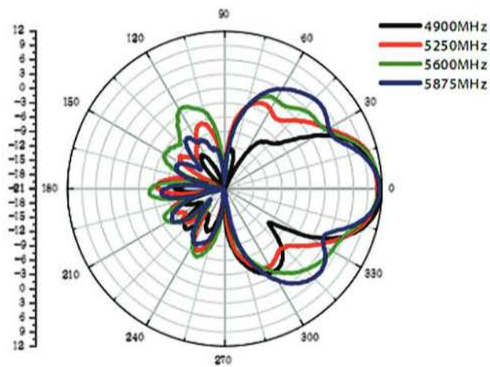
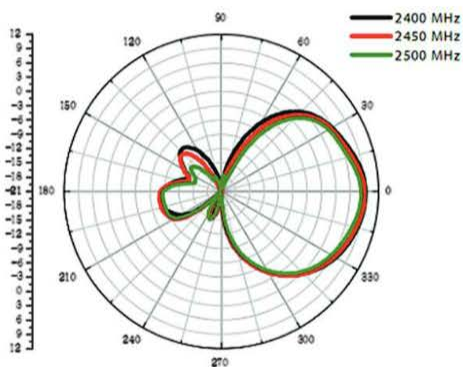
Рис. 1.29. Антенна ANT24-2100



Рис. 1.30. Антенна ANT70-1800



а



б

Рис. 1.31. Диаграммы направленности антенны ANT70-1800 в горизонтальной (а) и вертикальной (б) плоскости

стандарта 802.11 также можно разделить на антенны диапазона 2,4 ГГц, диапазона 5 ГГц и многодиапазонные антенны, способные работать в обоих диапазонах.

По назначению антенны можно разделить на *комнатные* и *уличные*. Как следует из названия, комнатные антенны предназначены для использования внутри помещений. Уличные антенны служат для использования вне помещений и обладают большим коэффициентом усиления для покрытия большей области пространства. Следовательно, использование таких антенн внутри помещения несет опасность сильного облучения присутствующих там людей. Кроме того, к внешним антеннам предъявляются дополнительные конструктивные требования по обеспечению возможности их эффективной работы в условиях сильного ветра, осадков (снег, дождь, град) и изменения температуры окружающей среды.

По исполнению антенны беспроводных устройств можно разделить на *встроенные* в радиомодуль устройства и *съёмные*. Встроенную в устройство антенну заменить нельзя. Например, встроенные антенны имеют ноутбуки, смартфоны и планшеты. Съёмные антенны подключаются к беспроводным устройствам с помощью специальных разъемов (чаще всего в беспроводных устройствах используются разъемы SMA- и N-типа). Такие антенны можно отключать и заменять другими, обладающими требуемыми характеристиками. При замене антенны требуется убедиться, что она имеет разъем необходимого для подключаемого устройства типа.

По исполнению антенны также можно разделить на *внешние* и *внутренние*. Внутренние антенны скрыты корпусом беспроводного устройства, что защищает их от повреждений, уменьшает размеры и улучшает дизайн устройства. Однако большое влияние на излучение антенны, а следовательно, и на форму диаграммы направленности оказывают металлические предметы, расположенные в непосредственной близости от антенны. Поэтому диаграммы направленности встроенных антенн точек доступа, мобильных устройств, планшетов и нетбуков имеют искаженную форму и их максимум смещен относительно нормали к антенне.

Для примера представим двухдиапазонную антенну M2450DLNТF компании Airgain, применяющуюся в различных беспроводных устройствах (рис. 1.32). Диаграммы направленности этой антенны показаны на рис. 1.33. Искажения диаграммы направленности возникают вследствие близко расположенных к антеннам проводников, металлических радиаторов и т. п. Для их устранения рекомендуется по возможности убрать металлические предметы в радиусе 1 м от антенны.

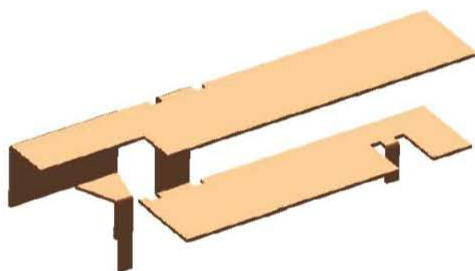


Рис. 1.32. Антенна M2450DLNТF компании Airgain

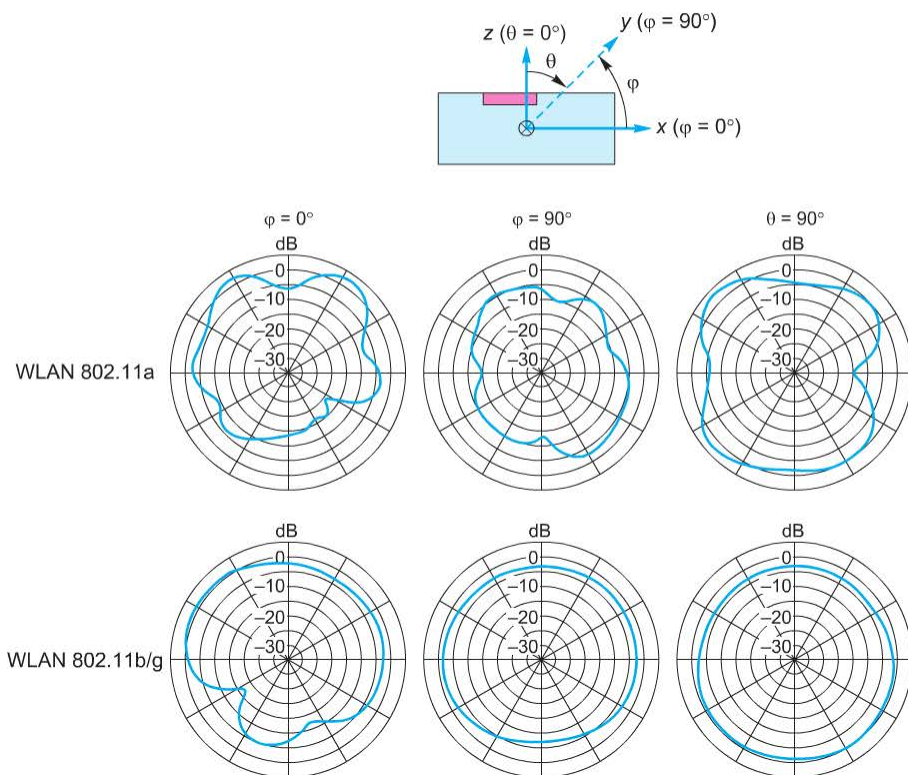


Рис. 1.33. Диаграммы направленности антенны M2450DLNTF

Антенные решетки

Отдельным классом антенн являются антенные решетки, представляющие собой антенны, состоящие из нескольких, обычно однотипных, излучателей, определенным образом расположенных в пространстве. Антенные решетки могут быть построены на основе любых описанных выше типов антенн. Объединение нескольких антенн в решетку наделяет такую конструкцию дополнительными свойствами и способностями. Например, антенная решетка из ненаправленных антенн при правильном расстоянии между элементами способна быть направленной, что позволяет получить высокий коэффициент усиления. Если определенным образом управлять фазами токов элементов антенны, то можно изменять положение максимума ДН антенны (т. е. осуществлять электрическое сканирование в пространстве без поворота антенны) и форму самой ДН (проводить адаптацию ДН, например, для отстройки от радиопомех других беспроводных устройств). Однако наличие перечисленных свойств сильно усложняет конструкцию антенны и системы формирования и обработки сигнала, и потому они не находят широкого применения в беспроводных устройствах.

Антенные решетки можно классифицировать по способам питания (соединения элементов между собой), по расположению элементов, по способам управления диаграммой направленности, по способам обработки сигнала. По способам питания решетки разделяются на антенны с последовательным, параллельным, комбинированным питанием. Рассмотрим подробнее лишь те конструкции антенных решеток, которые используются в сетях 802.11.



Рис. 1.34. Антенна ANT24-1202

Увеличить усиление штыревой антенны можно за счет дополнительных элементов, т. е. увеличения площади излучающей поверхности (эффективной площади антенны). Если располагать дополнительные элементы вдоль главной оси штыревой антенны, то получим так называемую коллинеарную (соосную) антенную решетку. Пример такой антенны показан на рис. 1.34. В антенне ANT24-1202 сигнальный ток от передатчика протекает по всей оси антенны и последовательно частично ответвляется в каждый ее элемент, т. е. такая антенная решетка запитывается последовательно и поэтому является решеткой с последовательным питанием.

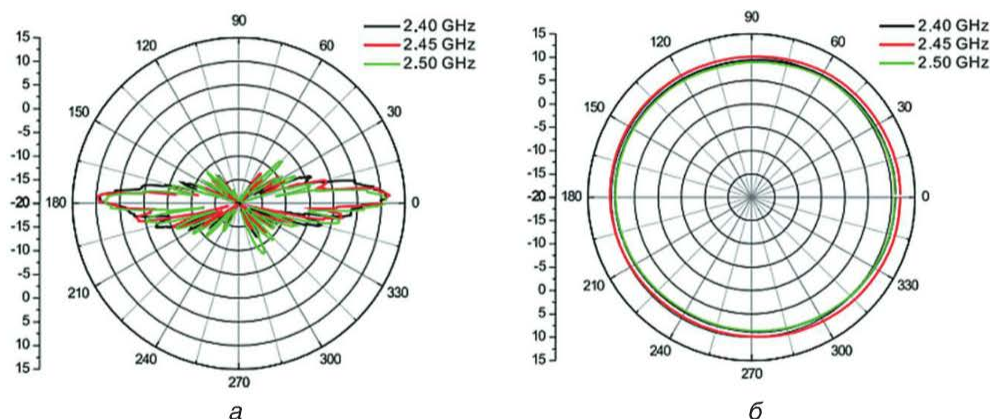


Рис. 1.35. Диаграммы направленности антенны ANT24-1202 в вертикальной (а) и горизонтальной (б) плоскостях

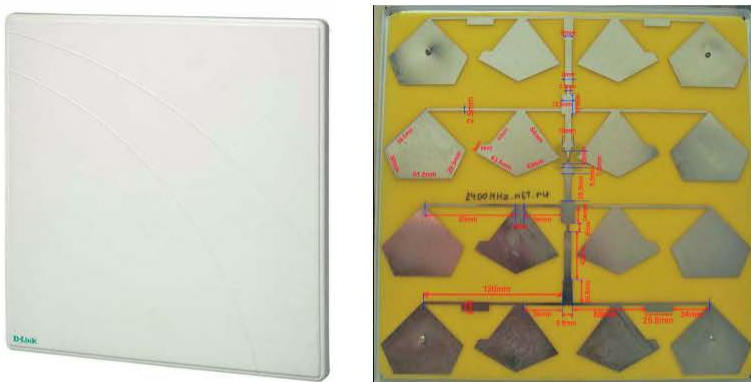


Рис. 1.36. Антенна ANT24-1800

Увеличение числа излучателей приводит к сужению ДН антенны и, как следствие, к увеличению коэффициента усиления в той плоскости, где расположены излучатели (рис. 1.35).

Примером печатной микрополосковой антенной решетки является ANT24-1800, показанная на рис. 1.36. Как видно из рисунка, антенна изготовлена по технологии печатных плат на диэлектрической пластине с излучателями многоугольной формы. Для питания антенны используется комбинированная последовательно-параллельная схема.

Антенны MIMO

MIMO — технология пространственного кодирования сигнала, позволяющая увеличить полосу пропускания канала, в котором передача данных и их прием осуществляются системами из нескольких антенн. Расширение полосы пропускания происходит за счет того, что каждая из антенн передает свой информационный сигнал в отдельном пространственном потоке. Максимальная эффективность системы MIMO достигается при независимости пространственных каналов между собой, т. е. когда сигнал, передаваемый по одному потоку, не влияет или слабо влияет на сигнал, передаваемый по другому. Увеличение независимости пространственных каналов достигается за счет пространственного разнесения антенн, а также применения разной поляризации для разных каналов. Передающие и приемные антенны разносят так, чтобы корреляция между сиг-

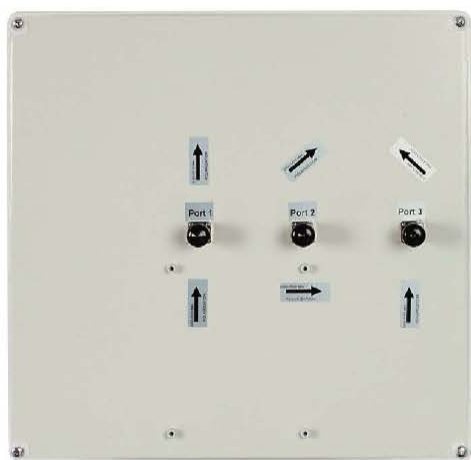


Рис. 1.37. Антенна ANT70-1400N

налами соседних антенн была слабой. Например, за счет использования линейной горизонтальной и вертикальной поляризации можно создать два независимых канала для системы ММО.

Таким образом, для построения системы ММО размером $m \times n$ необходимо иметь m передающих и n приемных антенн. Число пространственных потоков определяется минимальным числом антенн на одной из сторон связи. Примером такой антенны является ANT24-0230, позволяющая создать систему ММО с тремя пространственными потоками (см. рис. 1.22). На рис. 1.37 показана антенна ANT70-1400N, выполненная по печатной полосковой технологии и позволяющая создать систему ММО с тремя пространственными потоками, разделяемыми по поляризации в диапазонах 2,4 и 5 ГГц. Подробнее про систему ММО см. 5.6 «Спецификация IEEE 802.11n».

1.3. Преобразование единиц измерения

При расчете различных параметров беспроводных сетей часто приходится выполнять преобразование одних единиц измерения в другие. Проблема состоит в том, что в технических описаниях и законодательных актах, регулирующих использование радиочастотного спектра в России, присутствуют как линейные (ватты), так и логарифмические (децибелы) единицы измерения.

Децибелы являются логарифмическими единицами измерения уровней мощности, затухания и усиления сигналов. В децибелах принято измерять затухание волн при распространении их в поглощающей среде, коэффициент усиления антенны, отношение сигнал/шум. Русское обозначение единицы «децибел» — «дБ», международное — «dB».

Децибел является безразмерной относительной величиной, предназначенной для измерения отношения двух одноименных величин с применением к полученному отношению логарифмического масштаба.

Для выражения абсолютных значений мощности используются единицы дБм (dBm) и дБВт (dBW). Для этого достаточно условиться, какой уровень измеряемой физической величины будет принят за базовый (условный ноль дБ). В дБм обычно выражается мощность передатчиков. За нулевой уровень дБм принята мощность в 1 мВт (mW). Для перевода мощности из мВт в дБм необходимо выполнить следующее вычисление:

$$P_{dBm} = 10 \lg \frac{P_{mW}}{1mW},$$

где P_{dBm} — мощность передатчика, выраженная в дБм, P_{mW} — мощность передатчика, выраженная в мВт.

Например, чтобы перевести мощность, равную 400 мВт, в дБм, надо выполнить следующие действия:

$$10 \lg \frac{400}{1} = 26 \text{ дБм.}$$

Обратное преобразование из дБм в мВт выполняется по формуле

$$P_{mW} = 10^{\frac{P_{dBm}}{10}}.$$

Чтобы перевести мощность, равную 16 дБм, в мВт, надо произвести следующее вычисление:

$$10^{\frac{16}{10}} \cong 40 \text{ мВт}.$$

В табл. 1.1 приведены значения мощности сигналов, выраженных в дБм и мВт.

Таблица 1.1. Перевод мощности сигналов из дБм в мВт

дБм	мВт	дБм	мВт	дБм	мВт
0	1,0	11	13	21	126
1	1,3	12	16	22	158
2	1,6	13	20	23	200
3	2,0	14	25	24	251
4	2,5	15	32	25	316
5	3,2	16	40	26	398
6	4,0	17	50	27	501
7	5,0	18	63	28	631
8	6	19	79	29	794
9	8	20	100	30	1 000
10	10				

В дБВт (dBW) за нулевой уровень принята мощность в 1 Вт (W). Формулы для перевода аналогичны вышеприведенным с той разницей, что в качестве нулевого уровня выбрана величина 1 Вт, а измеренная мощность также должна быть выражена в ваттах.

dBi (дБи) — изотропный децибел (децибел относительно изотропного излучателя). Характеризует коэффициент усиления антенны относительно коэффициента направленного действия изотропного излучателя. Как правило, если не оговорено специально, характеристики усиления реальных антенн даются именно относительно усиления изотропного излучателя, т. е. если говорят, что коэффициент усиления некой антенны равен 12 децибелам, подразумевается 12 дБи.

Как уже упоминалось ранее, децибелы являются нелинейными единицами измерения. Поэтому когда говорят, например, об удвоении мощности, равной 100 мВт (20 дБм), это не означает, что мощность увеличится до 40 дБм: 40 дБм соответствует 10 000 мВт. Поэтому для расчетов полезно запомнить соответствие:

- увеличение мощности в мВт в 1,26 раза эквивалентно прибавлению к мощности в дБм 1 дБ. Уменьшение мощности в мВт в 1,26 раза эквивалентно вычитанию из мощности в дБм 1 дБ;
- увеличение мощности в мВт в 2 раза эквивалентно прибавлению к мощности в дБм 3 дБ. Уменьшение мощности в мВт в 2 раза эквивалентно вычитанию из мощности в дБм 3 дБ;
- увеличение мощности в мВт в 10 раз эквивалентно прибавлению к мощности в дБм 10 дБ. Уменьшение мощности в мВт в 10 раз эквивалентно вычитанию из мощности в дБм 10 дБ.

Приведем пример. Пусть выходная мощность передатчика равна 100 мВт (20 дБм). Если мы увеличиваем мощность в 2 раза до 200 мВт, то должны сложить 20 дБм и 3 дБм и получим мощность 23 дБм. Если мощность уменьшится в 2 раза до 50 мВт, то мощность в дБм будет равна $20 - 3 = 17$ дБм.

2. Стандарт беспроводных локальных сетей IEEE 802.11

2.1. Архитектура IEEE 802.11

Институт инженеров электротехники и электроники IEEE сформировал рабочую группу по стандартам для беспроводных локальных сетей 802.11 в 1990 году. Она занималась разработкой всеобщего стандарта для радиооборудования и сетей, работающих на частоте 2,4 ГГц со скоростями доступа 1 и 2 Мбит/с. Работы по созданию стандарта были завершены через 7 лет, и в июне 1997 года была ратифицирована первая спецификация 802.11.

Стек протоколов стандарта IEEE 802.11 соответствует общей структуре стандартов комитета 802, т. е. состоит из физического уровня и канального уровня с подуровнями управления доступом к среде MAC (*Media Access Control*) и логической передачи данных LLC (*Logical Link Control*). Как и у всех технологий семейства 802, технология 802.11 определяется двумя нижними уровнями, т. е. физическим уровнем и подуровнем MAC, а подуровень LLC выполняет стандартные для всех технологий локальных сетей функции.

На физическом уровне существует несколько вариантов спецификаций, отличающихся используемым частотным диапазоном, методом кодирования и, как следствие, — скоростью передачи данных. Все варианты спецификаций физического уровня работают с одним и тем же алгоритмом доступа к среде передачи, определенном на MAC-подуровне, но некоторые временные параметры MAC-подуровня зависят от используемого физического уровня (рис. 2.1).

Канальный уровень	IEEE 802.1: аутентификация (802.1X)					
	LLC (Logical Link Control)					
	MAC – Media Access Control					
Физический уровень	802.11	802.11a	802.11b	802.11g	802.11n	802.11ac
	FHSS, DSSS PHY	OFDM PHY	HR/DSSS PHY	ERP PHY	HT PHY	VHT PHY

Рис. 2.1. Стек протоколов IEEE 802.11

Основным строительным блоком беспроводных сетей стандарта IEEE 802.11 является базовый набор услуг (*Basic Service Set, BSS*), который состоит из нескольких станций (*station, STA*), реализующих общий протокол MAC и состоящих за доступ к разделяемой среде передачи данных. Зона покрытия, внутри которой станции, являющиеся членами BSS, остаются на связи, называется базовой зоной обслуживания (*Basic Service Area, BSA*). Если

какая-либо станция выходит из зоны обслуживания, то она уже не может напрямую взаимодействовать со станциями, оставшимися в ней. BSS может быть изолирован или соединен с магистральной распределительной системой (*Distribution system*) через точку доступа (*Access point*).

Основные термины IEEE 802.11

Станция (*Station*) — любое устройство, физический уровень и MAC-подуровень которого соответствуют стандарту IEEE 802.11.

Точка доступа (*Access point*) — любой объект, обладающий функциональными возможностями станции и обеспечивающий доступ к распределительной системе посредством беспроводной среды.

Базовый набор услуг (*Basic Service Set, BSS*) — набор станций, которыми управляет одна функция координации.

Функция координации (*Coordination function*) — логическая функция, определяющая логику, по которой станция, функционирующая внутри базового набора услуг, может передавать блок данных протокола (*Protocol Data Unit, PDU*) через беспроводную среду.

Распределительная система (*Distribution System, DS*) — система, используемая для соединения нескольких базовых наборов услуг и интеграции проводной локальной сети в расширенный набор услуг.

Расширенный набор услуг (*Extended Service Set, ESS*) — два или большее число базовых наборов услуг, соединенных распределительной системой. Для подуровня LLC любой станции, ассоциированной с одним из этих базовых наборов услуг, расширенный набор услуг представляется единым логическим базовым набором услуг.

В BSS передача данных между клиентскими станциями выполняется через точку доступа независимо от того находятся станция-отправитель и станция-получатель в одном или разных BSS. При передаче кадров от одной станции другой в пределах одного BSS станция-отправитель сначала пересылает кадры точке доступа, которая затем направляет кадры нужному адресату. Если станция-получатель находится в другом BSS, станция-отправитель посылает кадры точке доступа, которая перенаправляет их через распределительную систему в направлении станции-получателя. Распределительная система может быть коммутатором, проводной или беспроводной сетью. Режим работы BSS, при котором все операции выполняются через точку доступа, называется инфраструктурным (*Infrastructure*) (рис. 2.2).

Для ситуации, когда в BSS все станции являются мобильными устройствами (ноутбуками, планшетами, телефонами и т.д.), в IEEE 802.11 определен режим работы, при котором они могут взаимодействовать друг с другом напрямую без использования точек доступа. Такой BSS называется независимым BSS (*Independent Basic Service Set, IBSS*), а режим работы мобильных станций — *ad hoc* (лат. *к случаю*) (рис. 2.3). Следует отметить, что в режиме *ad hoc* могут работать только беспроводные адаптеры.

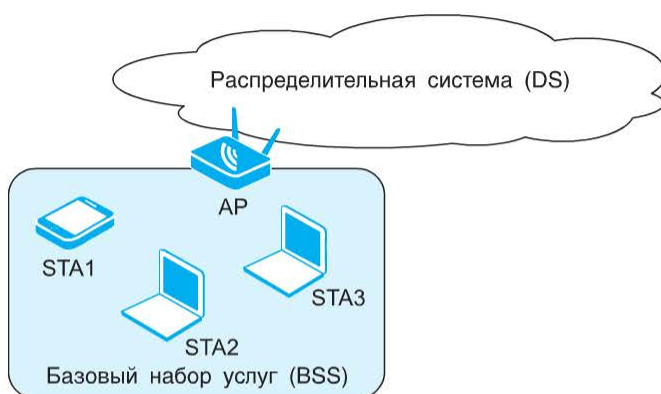


Рис. 2.2. Базовый набор услуг IEEE 802.11 (инфраструктурный режим)

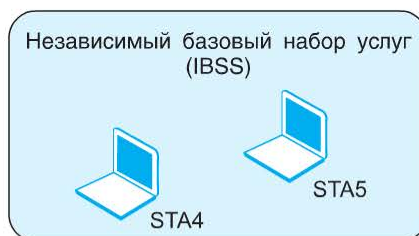
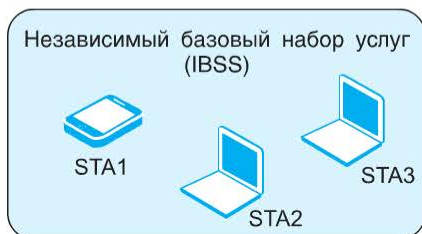


Рис. 2.3. Независимый базовый набор услуг IEEE 802.11 (режим *ad hoc*)

IBSS представляет собой одноранговую беспроводную сеть, состоящую из двух или нескольких станций, которые могут устанавливать соединение «точка-точка» непосредственно друг с другом. Данный тип беспроводной сети не требует предварительного планирования и обычно создается на непродолжительное время (по необходимости, «к случаю»), например, чтобы передать какой-нибудь файл с планшета на планшет, телефон или ноутбук. Поэтому другое, часто встречающееся название такой архитектуры беспроводной сети, — *ad hoc network*. Независимым BSS называется потому, что создается только одна зона обслуживания, не имеющая интерфейса для подключения к распределительной системе.

Внимание: в настройках беспроводного адаптера предусмотрена возможность выбора режима работы — *ad hoc* или Infrastructure. Точка доступа всегда работает только в инфраструктурном режиме.

Членство станций в BSS является динамическим. Станции могут отключаться, выходить из зоны обслуживания и входить в нее. Области обслуживания BSS могут перекрываться, так что одна станция может входить в зоны действия нескольких BSS. Однако для того, чтобы получать все сервисы, обеспечиваемые беспроводной сетью, станция должна быть ассоциирована с соответствующим BSS.

Для того чтобы клиентская станция могла отличить один BSS от другого, каждый BSS уникально определяется идентификатором базового набора услуг (*Basic Service Set Identifier, BSSID*). Для BSS, работающего в инфраструктурном режиме, BSSID является MAC-адресом точки доступа. Для BSS, работающего в режиме *ad hoc*, BSSID является локально администрируемым MAC-адресом, генерируемым произвольным образом. BSSID всегда ассоциируется только с одним BSS и указывается в заголовке кадра данных.

Идентификатор набора услуг (*Service Set Identifier, SSID*) является удобным для восприятия и запоминания человеком именем беспроводной сети. В отличие от BSSID, который всегда идентифицирует только один BSS, SSID идентифицирует всю беспроводную сеть (рис. 2.4). Такая сеть может состоять как из одного BSS или IBSS, так и из нескольких BSS, объединенных с помощью распределительной системы. Идентификатор SSID представляет собой чувствительную к регистру текстовую строку длиной до 32 байт. Для того чтобы устройства могли взаимодействовать друг с другом, в настройках всех устройств, подключенных к одной беспроводной сети, должен быть указан одинаковый идентификатор SSID.

Беспроводные клиентские устройства могут автоматически определять все беспроводные сети, в зоне действия которых они находятся, так как значение SSID

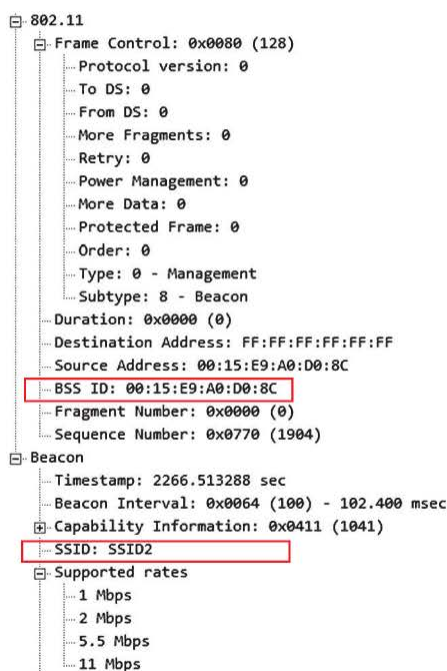


Рис. 2.4. Идентификаторы SSID и BSSID

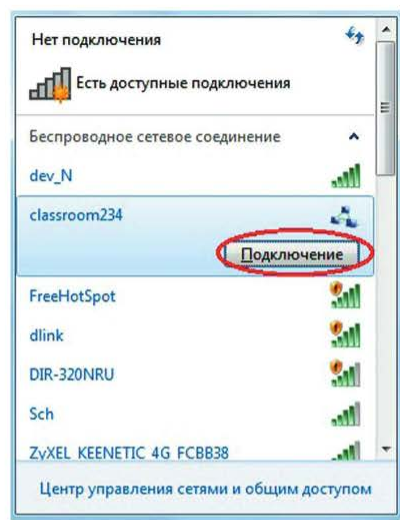


Рис. 2.5. Список беспроводных сетей (в интерфейсе ОС Windows 7), обнаруженных беспроводным адаптером

содержится в сигнальных (маячковых) кадрах (*Beacon frame*), которые ширококестельно рассылаются точкой доступа по сети, как только она становится активной. Выбрав из списка имя нужной беспроводной сети, пользователь может подключить к ней свое устройство (рис. 2.5).

В оборудовании D-Link в качестве SSID по умолчанию используется имя «dlink». Это имя можно изменить, указав новое значение SSID в настройках точки доступа или беспроводного маршрутизатора (рис. 2.6).

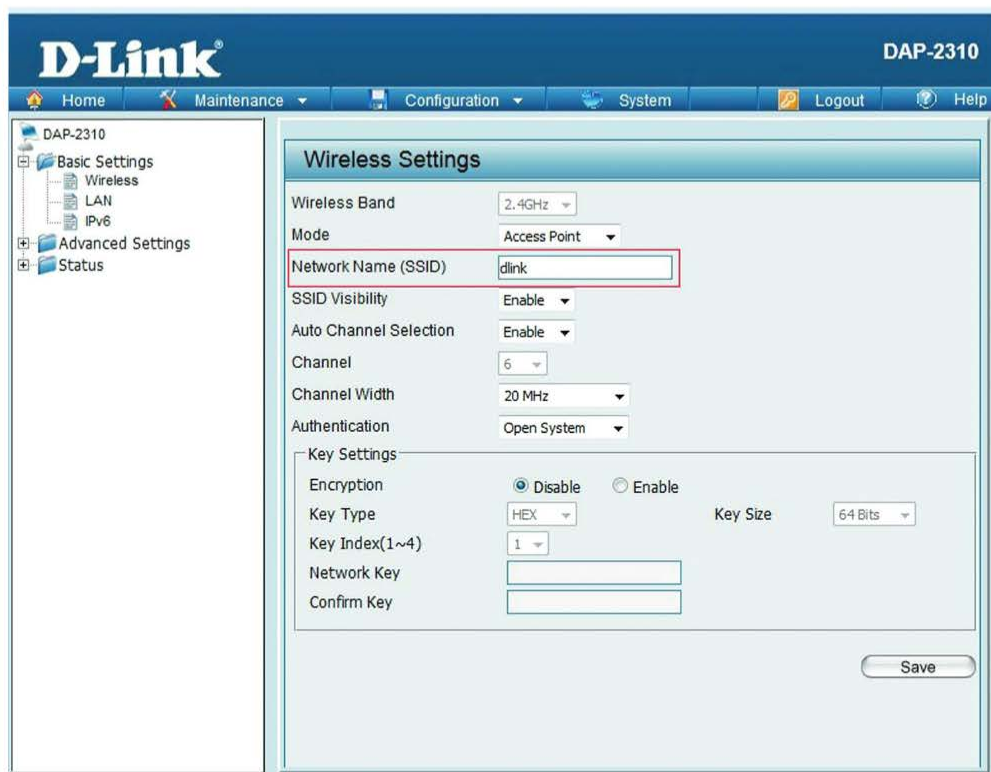


Рис. 2.6. Настройка SSID на точке доступа D-Link DAP-2310

Идентификатор SSID, рассылаемый точками доступа и беспроводными маршрутизаторами в ширококестельных сигнальных кадрах, по умолчанию виден всем клиентским устройствам, находящимся в их зоне действия. Для предотвращения случайного или намеренного подключения посторонних клиентских устройств к беспроводной сети ее SSID можно сделать невидимым (скрыть) для клиентского оборудования путем соответствующих настроек параметров точки доступа или маршрутизатора (рис. 2.7). После активации настроек в рассылаемых устройствами сигнальных кадрах значение SSID отображаться не будет (рис. 2.8).

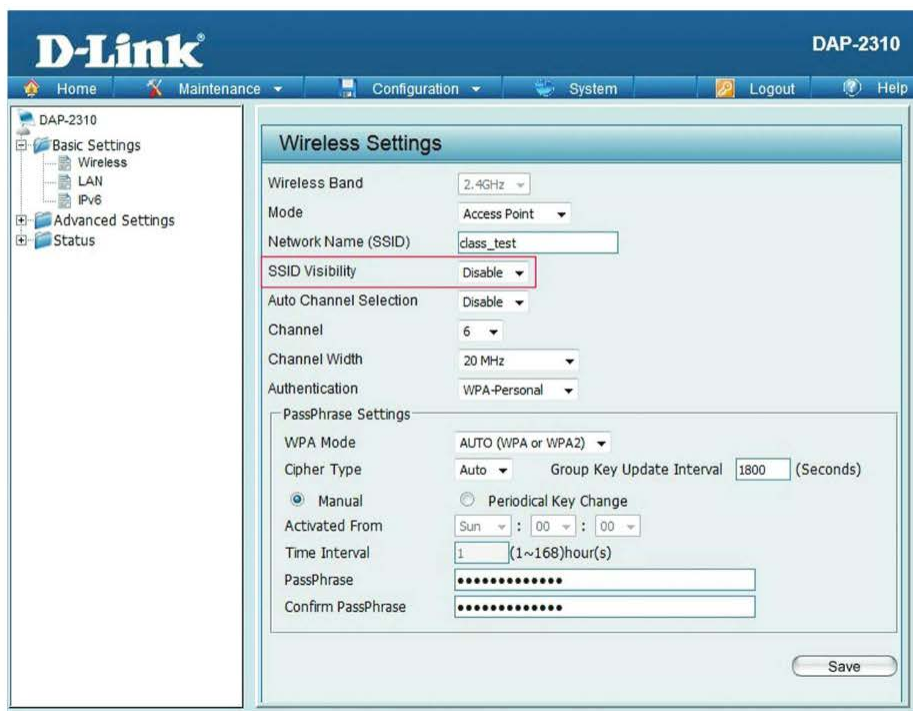


Рис. 2.7. Отключение видимости SSID на точке доступа D-Link DAP-2310

Внимание: идентификатор SSID не является средством обеспечения безопасности и альтернативой парольной защите. Он служит только для идентификации беспроводных сетей.

Устройства, работающие под управлением ОС Windows 7 и выше, обнаруживают все сети, в радиусе действия которых они находятся, даже если идентификатор SSID скрыт. Информация о SSID включается в пакеты данных, запросы ассоциации/повторной ассоциации, кадры пробного запроса/ответа, и поэтому беспроводная сеть может быть обнаружена с помощью анализатора сетевого трафика.

В том случае, если в списке беспроводных соединений клиентского устройства отсутствует нужная беспроводная сеть (например, SSID сети скрыт), идентификатор SSID сети можно вручную ввести в настройках этого устройства (рис. 2.9).

Распределительная система и инфраструктурные BSS позволяют создавать беспроводные сети любой протяженности и сложности (рис. 2.10). В стандарте IEEE 802.11 такие сети называются расширенный набор услуг (*Extended Service Set, ESS*). ESS состоит из двух и более инфраструктурных BSS с одним именем SSID, соединенных распределительной системой (рис. 2.11). Распределительная система не входит в состав ESS. Все станции внутри ESS могут взаимодействовать друг с другом, а мобильные станции могут переходить из одного BSS в другой в пределах ESS, не теряя связи с сетью.

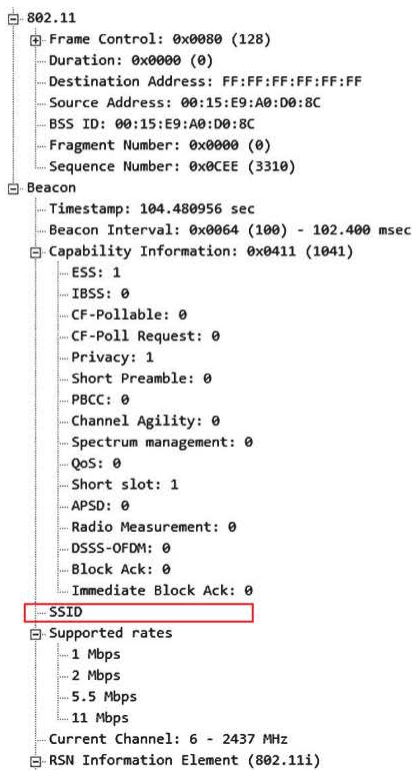


Рис. 2.8. Сигнальный кадр со скрытым SSID

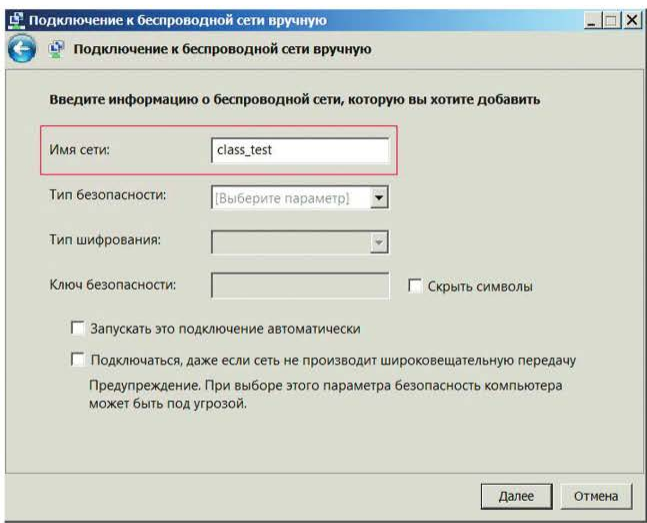


Рис. 2.9. Подключение к беспроводной сети с ручным заданием параметров в интерфейсе ОС Windows 7

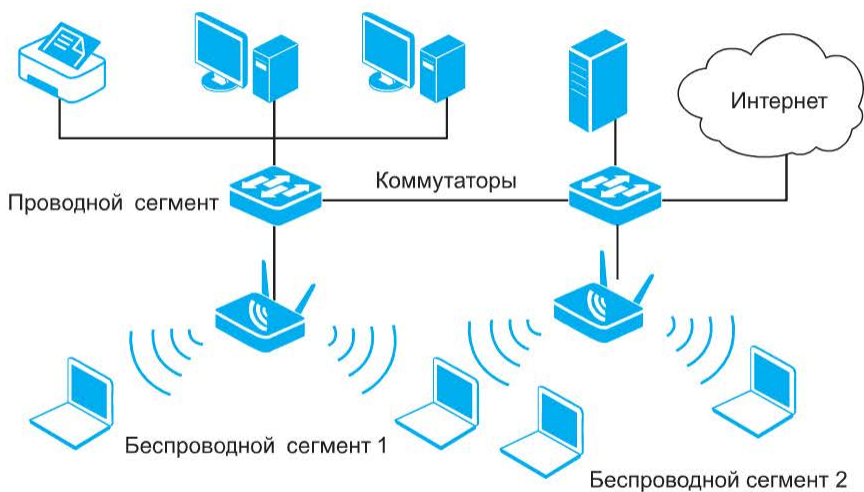


Рис. 2.10. Пример беспроводной сети с инфраструктурой

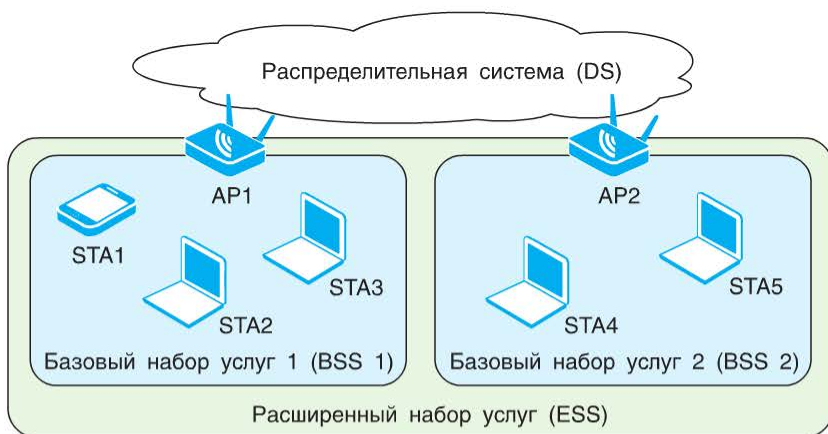


Рис. 2.11. Расширенный набор услуг IEEE 802.11

Для интеграции архитектуры IEEE 802.11 с проводной сетью используется портал. Логика портала реализуется в устройстве, таком, как коммутатор или маршрутизатор, являющемся частью проводной локальной сети и присоединенном к распределительной системе (рис. 2.12).

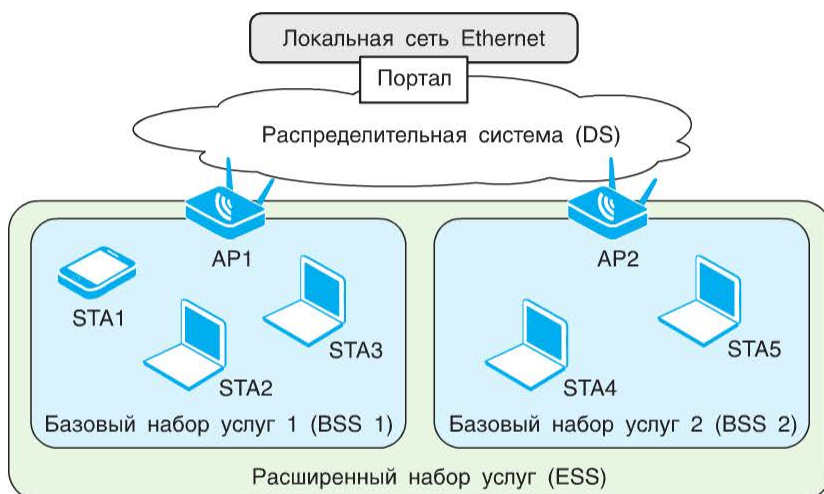


Рис. 2.12. Подключение беспроводной сети к проводной локальной сети

2.2. Услуги IEEE 802.11

Стандарт IEEE 802.11 определяет набор услуг (сервисов), которые должна предлагать беспроводная сеть для обеспечения возможностей, аналогичных функциям проводных сетей. Весь набор разделен на две группы: услуги, предоставляемые станцией, и услуги, предоставляемые распределительной системой.

Услуги первой группы реализуются на каждой станции 802.11, в том числе на станциях, являющихся точками доступа:

- аутентификация;
- отмена аутентификации;
- конфиденциальность данных;
- доставка MSDU;
- динамический выбор частоты (DFS);
- управление мощностью передатчика (TPC);
- синхронизация таймеров верхнего уровня;
- планирование трафика (качество обслуживания, QoS);
- радиочастотные измерения;
- динамическое разблокирование станции (DSE).

Услуги распределительных систем предлагаются между базовыми наборами услуг (BSS). Эти услуги могут быть реализованы на точках доступа или других специализированных устройствах, подключенных к распределительной системе:

- ассоциация;
- разрыв ассоциации;
- распределение;
- интеграция;

- повторная ассоциация;
- планирование трафика (QoS);
- динамическое разблокирование станции (DSE).

Шесть из перечисленных услуг используются для организации доставки **блоков данных сервиса MAC** (MAC Service Data Unit, MSDU) от станции к станции. Три услуги используются для управления доступом к беспроводной сети и обеспечения конфиденциальности. Две услуги используются для управления спектром частот. Одна из услуг предназначена для реализации обслуживания трафика. Существует услуга для синхронизации таймеров верхнего уровня. Также поддерживается услуга, позволяющая выполнять радиочастотные измерения.

Термины, описывающие блоки передаваемых данных

Блок данных протокола MAC (MAC Protocol Data Unit, MPDU) — модуль данных, которым обмениваются два одноранговых объекта MAC, используя услуги физического уровня.

Блок данных сервиса MAC (MAC Service Data Unit, MSDU) — информация, передаваемая единым блоком между пользователями MAC; обычно это PDU уровня LLC.

Формат блоков MPDU и MSDU показан на рис. 2.13.

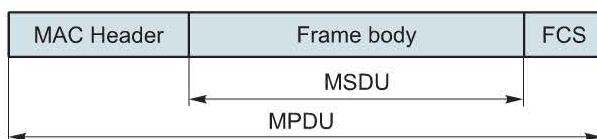


Рис. 2.13. Взаимосвязь MSDU и MPDU

Для реализации каждой из услуг используется один или несколько типов кадров MAC. MAC-подуровень стандарта IEEE 802.11 поддерживает три типа кадров — кадры данных, кадры управления и контрольные кадры. Описания услуг в соответствии со стандартом IEEE 802.11-2012 приведены далее.

2.2.1. Распределение сообщений в пределах распределительной системы

В распределении сообщений в пределах распределительной системы задействованы две услуги: *распределение (distribution)* и *интеграция (integration)*.

Распределение является основной услугой, используемой станциями для обмена кадрами в пределах ESS (когда кадр должен пройти через распределительную систему, чтобы проследовать от станции из одного BSS к станции, находящейся в другом BSS). Обратимся к рис. 2.12 и предположим, что требуется передать кадр от станции STA1 к станции STA4. Станция STA1 передает кадр точке доступа AP1 (входная точка доступа), которая пересылает кадр распределительной системе. Предположим, что в качестве распределительной

тельной системы выступает коммутатор. Далее распределительная система направляет кадр к точке доступа AP2 (выходная точка доступа) целевого BSS, которая принимает его и передает станции STA4. Логика передачи сообщения через распределительную систему в стандарте IEEE 802.11 не описывается. Однако стандарт требует, чтобы распределительная система получала информацию о станциях в пределах ESS. Эта информация предоставляется распределительной системе через услуги ассоциации. При обмене данными двух станций в пределах одного BSS услуга распределения предоставляется точкой доступа этого BSS.

Услуга интеграции позволяет передавать данные между станцией беспроводной сети и станцией проводной локальной сети, которая физически соединена с распределительной системой. Услуга интеграции решает все вопросы обмена данными, связанные с логикой трансляции адресов и преобразования среды.

2.2.2. Услуги, связанные с ассоциацией

Основной задачей MAC-подуровня является передача MSDU между объектами MAC-подуровня. Выполняет эту задачу распределительная система, для функционирования которой требуется информация о станциях в пределах ESS. Эта информация предоставляется услугами, связанными с ассоциацией. Перед тем как распределительная система сможет передавать или принимать данные от станции, станция должна установить *ассоциацию*.

Для того чтобы понять концепцию ассоциации, необходимо сначала описать понятие мобильности, которое в стандарте определяется тремя типами перехода:

- без перехода: станция либо стационарна (*static*), либо перемещается в пределах досягаемости станций, принадлежащих к тому же BSS (*local movement*);
- переход BSS: переход станции из одного BSS в другой в пределах одного ESS. В этом случае для доставки данных требуется найти новое местоположение станции;
- переход ESS: перемещение станции из BSS одного ESS в BSS другого ESS. При переходе этого типа сохранность соединений высшего уровня, поддерживаемых сетью 802.11, не гарантируется. Фактически наиболее вероятным следствием такого перехода является разрыв соединения.

Для доставки сообщения в пределах распределительной системы услуге распределения должно быть известно, где расположена станция-адресат. В частности, распределительная система должна знать, какая станция выступает в роли точки доступа, т. е. кому передать данные, предназначенные станции-адресату. Для этого станция должна поддерживать ассоциацию с точкой доступа в пределах текущего BSS. С этим требованием связаны три услуги:

- ассоциация (*association*): установление первоначального соединения между станцией и точкой доступа. Перед тем как станция начнет передавать

или получать кадры в беспроводной локальной сети, ее нужно идентифицировать. Для этого станция должна установить ассоциацию с точкой доступа в пределах конкретного BSS. Следует отметить, что станция может установить ассоциацию *только с одной* точкой доступа, в то время как точка доступа может быть одновременно ассоциирована с множеством станций. Для облегчения маршрутизации и адресной доставки сообщений точка доступа может передавать информацию об ассоциированных с ней станциях другим точкам доступа данного ESS;

- повторная ассоциация (*reassociation*): передача установленной ассоциации между точками доступа для предоставления мобильной станции возможности переходить из одного BSS в другой в пределах ESS;
- разрыв ассоциации (*disassociation*): уведомление от станции или точки доступа об аннулировании существующей ассоциации. Станция должна получить это уведомление до выхода из ESS или отключения.

2.2.3. Услуги управления доступом и обеспечения безопасности

В проводных сетях, где станции физически подключаются к сети с помощью кабельной проводки, имеется возможность контролировать эти подключения. Беспроводная среда передачи является физически общедоступной, поэтому возникает проблема контроля над подключением к беспроводной сети. Для того чтобы предоставлять функциональность управления доступом, эквивалентную проводной локальной сети, стандарт IEEE 802.11 требует наличия в беспроводных сетях таких сервисов, как *аутентификация* и *конфиденциальность* данных.

Основные термины систем безопасности

Аутентификация (*Authentication*) — сервис безопасности, который обеспечивает подтверждение того, что информация получена от законного источника требуемым получателем.

Идентификация (*Identification*) — сервис, с помощью которого определяются уникальные свойства пользователей, позволяющие отличать их друг от друга, и способы, с помощью которых пользователи указывают свои идентификационные сведения информационной системе. Идентификация тесно связана с аутентификацией.

Авторизация (*Authorisation*) — предоставление полномочий (прав и разрешений) доступа. Права и разрешения, предоставленные индивидууму (субъекту) или процессу, обеспечивают возможность доступа к требуемому ресурсу. После того как пользователь аутентифицирован, в процессе авторизации определяются права, доступные пользователю.

Конфиденциальность данных (*Data confidentiality*) — сервис безопасности, предназначенный для предотвращения пассивных атак на передаваемые или хранимые данные. Данный сервис обеспечивает недоступность информации неавторизованным пользователям.

Целостность данных (*Data integrity*) — сервис безопасности, обеспечивающий невозможность изменения данных без обнаружения факта этого изменения.

Пассивная атака (*Passive attack*) — атака, при которой злоумышленник не имеет возможность модифицировать передаваемые или хранимые данные и вставлять в информационный канал между отправителем и получателем свои сообщения. Целью пассивной атаки может быть только прослушивание передаваемых сообщений и анализ трафика.

В стандарте IEEE 802.11 управление доступом к беспроводной сети определено через услугу аутентификации, используемую станциями для идентификации себя в среде взаимодействующих станций. Стандарт определяет несколько методов аутентификации: аутентификацию открытых систем (*Open System authentication*), аутентификацию с общим ключом (*Shared Key authentication*), аутентификацию при быстром переходе BSS (*FT authentication*), аутентификацию на основе стандарта IEEE 802.1X-2004, аутентификацию на основе предварительно установленных ключей (*Pre-Shared key, PSK*). Стандарт не навязывает никаких обязательных методов аутентификации, поэтому на практике могут использоваться как небезопасные, так и надежные механизмы аутентификации. При этом обязательным условием ассоциации между станцией и точкой доступа является успешная аутентификация.

Услуга отмены аутентификации (*deauthentication*) используется станциями или точками доступа для отмены существующей аутентификации, что приводит к разрыву ассоциации.

В проводных сетях передавать и получать данные могут только те станции, которые физически подключены к сети. В беспроводных сетях передавать и получать данные может любая станция, находящаяся в пределах области охвата других устройств. Таким образом, проводная сеть обеспечивает некоторую конфиденциальность данных, ограничивая число возможных получателей устройствами, подключенными к сети. Для того чтобы приблизить уровень безопасности беспроводной сети к уровню безопасности проводной сети, стандарт IEEE 802.11 обеспечивает возможность защиты содержимого сообщений. Предотвращение чтения сообщений теми, кому они не предназначены, обеспечивается услугой конфиденциальности данных (*data confidentiality*).

Для обеспечения конфиденциальности и целостности данных стандарт предлагает (но не навязывает) использовать протоколы шифрования WEP, TKIP и CCMP. Протоколы WEP и TKIP основаны на алгоритме шифрования RC4, протокол CCMP основан на алгоритме AES (*Advanced Encryption Standard*). При этом стандарт не рекомендует использовать в современных сетях протокол WEP в связи с его криптографической уязвимостью.

Настройки конфиденциальности данных по умолчанию во всех беспроводных устройствах отсутствуют, т. е. по умолчанию защита данных не выполняется и они передаются в «чистом» (открытом) виде. Для того чтобы обеспечить конфиденциальность данных в беспроводной сети, на всех устройствах сети необходимо выполнить настройку параметров соответствующих протоколов безопасности.

2.3. Кадр MAC стандарта IEEE 802.11

Стандарт IEEE 802.11 описывает три типа кадров:

- *кадры данных* или *информационные кадры (data frames)* — используются для передачи данных;
- *контрольные кадры (control frames)* — служат для управления доступом к среде передачи данных;
- *кадры управления (management frames)* — используются для обмена управляющей информацией при выполнении таких операций подуровня MAC, как ассоциация и разрыв ассоциации, аутентификация и отмена аутентификации, синхронизация и др.

Рассмотрим общий формат кадра MAC. Каждый кадр MAC состоит из следующих основных компонентов: заголовок кадра, тело кадра переменной длины, контрольная сумма кадра. Общий формат кадра показан на рис. 2.14. Первые три поля («Управление кадром» (*Frame Control*)), «Длительность/идентификатор» (*Duration/ID*)), «Адрес 1» (*Address 1*)) и последнее поле («Контрольная сумма кадра» (*FCS*))) присутствуют во всех кадрах MAC. Остальные поля («Адрес 2» (*Address 2*)), «Адрес 3» (*Address 3*)), «Управление очередностью» (*Sequence Control*)), «Адрес 4» (*Address 4*)), «Управление QoS» (*QoS Control*)), «Тело кадра» (*Frame Body*)) присутствуют только в определенных кадрах MAC.

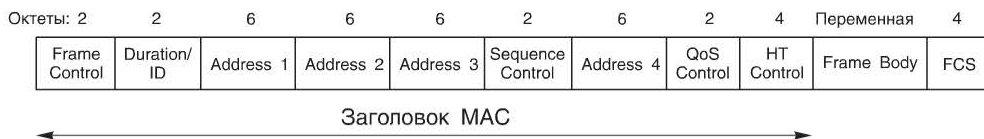


Рис. 2.14. Формат кадра MAC IEEE 802.11-2012

Каждый тип кадра разбивается на несколько подтипов в зависимости от выполняемой операции. Опишем поля общего формата кадра.

- *Управление кадром (Frame Control)*: поле состоит из 11 подполей и служит для указания типа и подтипа кадра и предоставления управляющей информации (формат поля описан ниже).
- *Длительность/идентификатор (Duration/ID)*: значение этого поля зависит от типа и подтипа кадра. Например, в кадрах данных и некоторых контрольных кадрах это поле содержит значение длительности соединения, которое используется для установки *вектора сетевого распределения NAV (Network Allocation Vector)*. В контрольных кадрах PS-Poll это поле содержит идентификатор ассоциации (*AID, Association ID*).
- *Адреса 1–4 (Address 1–4)*: четыре поля адреса используются для указания идентификатора BSSID, адреса источника (*SA, Source Address*), адреса назначения (*DA, Destination Address*), адреса передающей станции (*TA, Transmitter Address*) и адреса принимающей станции (*RA, Receiver Address*). Количество и значения полей адреса зависят от типа кадра.

- Управление очередностью (*Sequence Control*): это поле используется при фрагментации кадров и служит для определения порядка фрагментов, принадлежащих одному кадру, и предотвращения их дублирования. Оно состоит из двух подполей: «Номер фрагмента» (*Fragment Number*) длиной 4 бит, указывающего номер фрагмента кадра, и «Порядковый номер» (*Sequence Number*) длиной 12 бит, содержащего порядковый номер кадра.

- Управление QoS (*QoS Control*): это поле было добавлено в заголовок MAC после появления дополнения к стандарту IEEE 802.11e. Оно включает много подполей, содержащих различную информацию сервиса QoS, требуемую для обработки кадра. Два из них (*TID* и *Ack policy*) присутствуют во всех кадрах данных, имеющих поле QoS. Подполе *TID* (*Traffic Indicator*, *индикатор трафика*) указывает *класс трафика* (*traffic class*, *TC*) или *поток трафика* (*traffic stream*, *TS*), которому принадлежит блок данных сервиса MAC (MSDU), находящийся в поле «Тело кадра». Поле *Ack policy* идентифицирует политику отправки кадров подтверждения (ACK), используемую после доставки MSDU: *обычное подтверждение* (*normal acknowledgment*), *блочное подтверждение* (*block acknowledgment*), *без подтверждения* (*no acknowledgment*) и *неявное подтверждение* (*no explicit acknowledgment*). Остальные подполя поля управления QoS (*TXOP Limit*, *AP PS Buffer State*, *TXOP Duration Requested*, *Queue Size*, *EOSP* (*окончание периода сервиса*)) присутствуют только в кадрах определенного типа.

- Управление высокой пропускной способностью (*HT Control*): это поле было добавлено в заголовок кадра MAC после появления спецификации 802.11n. После принятия спецификации 802.11ac это поле стало иметь два варианта: HT и VHT. Оно всегда присутствует в кадре *упаковщика контрольных кадров* (*Control Wrapper*), а также в кадрах данных и кадрах управления с сервисом QoS, на что указывает бит «Порядок» поля «Управление кадром».

- Тело кадра (*Frame Body*): поле переменной длины, содержащее информацию, специфичную для каждого типа кадра. Минимальный размер этого поля 0 байт, максимальный размер определяется максимальными размерами блока данных сервиса MAC (MSDU), агрегированного MSDU (A-MSDU) и блока данных протокола MAC (MPDU), поддерживаемыми получателями; максимальной длительностью блока данных физического уровня; полями, присутствующими в заголовке MAC (QoS Control, HT Control); наличием шифрования данных.

- Контрольная сумма кадра (FCS): 32-битовое число проверки четности с избыточностью. Вычисляется на основе всех полей заголовка и поля «Тело кадра».

Внимание: в спецификациях 802.11a/b/g максимальный размер поля «Тело кадра» составляет 2304 байт (максимальный размер MSDU и MPDU). Максимальный размер поля «Тело кадра» спецификации 802.11n составляет 3839 или 7935 байт в зависимости от возможностей станции плюс накладные расходы на шифрование. Это связано с тем, что спецификация 802.11n поддерживает агрегацию кадров и максимальный размер поля «Тело кадра» ограничен максимальным размером A-MSDU. В спецификации 802.11ac максимальный размер поля «Тело кадра» ограничен максимальным размером MPDU и составляет 3839, 7935 или 11454 байт.

Опишем структуру двухбайтового поля «Управление кадром», состоящего из 11 подполей (рис. 2.15).

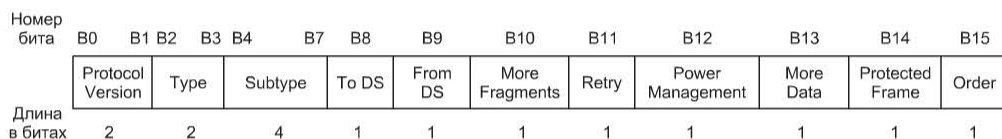


Рис. 2.15. Поле «Управление кадром»

- Версия протокола (*Protocol Version*): определяет версию протокола 802.11. Используемая в настоящее время версия протокола — 0. Остальные значения зарезервированы для будущего использования.

- Тип и подтип (*Type*, *Subtype*): вместе эти поля определяют назначение кадра: контроль, управление или данные. Каждый тип кадра имеет несколько подтипов, которые перечислены в табл. 2.1.

Таблица 2.1. Разрешенные комбинации типа и подтипа в поле «Управление кадром»

Тип		Подтип	
Значение типа	Описание типа	Значение подтипа	Описание подтипа
00	Управление	0000	Запрос ассоциации
00	»	0001	Ответ на запрос ассоциации
00	»	0010	Запрос повторной ассоциации
00	»	0011	Ответ на запрос повторной ассоциации
00	»	0100	Пробный запрос
00	»	0101	Ответ на пробный запрос
00	»	0110	Объявление синхронизации
00	»	0111	Зарезервировано
00	»	1000	Сигнальный кадр (Beacon)
00	»	1001	Объявление наличия трафика (ATIM)
00	»	1010	Разрыв ассоциации
00	»	1011	Аутентификация
00	»	1100	Отмена аутентификации
00	»	1101	Действие
00	»	1110	Действие без подтверждения
00	»	1111	Зарезервировано
01	Контроль	0000–0110	Зарезервировано
01	»	0111	Упаковщик контрольных кадров (Control Wrapper)

Тип		Подтип	
Значение типа	Описание типа	Значение подтипа	Описание подтипа
01	Контроль	1000	Запрос блочного подтверждения (Block-AckReq)
01	»	1001	Блочное подтверждение (BlockAck)
01	»	1010	PS-Poll
01	»	1011	RTS
01	»	1100	CTS
01	»	1101	ACK
01	»	1110	CF-End
01	»	1111	CF-End + CF-Ack
10	Данные	0000	Данные
10	»	0001	Данные + CF-Ack
10	»	0010	Данные + CF-Poll
10	»	0011	Данные + CF-Ack + CF-Poll
10	»	0100	Null (нет данных)
10	»	0101	CF-Ack (нет данных)
10	»	0110	CF-Poll (нет данных)
10	»	0111	CF-Ack + CF-Poll (нет данных)
10	»	1000	Данные с сервисом QoS
10	»	1001	Данные с сервисом QoS + CF-Ack
10	»	1010	Данные с сервисом QoS + CF-Poll
10	»	1011	Данные с сервисом QoS + CF-Ack + CF-Poll
10	»	1100	QoS Null (нет данных)
10	»	1101	Зарезервировано
10	»	1110	QoS CF-Poll (нет данных)
10	»	1111	QoS CF-Ack + CF-Poll (нет данных)
11	Зарезервировано	0000—1111	Зарезервировано

• Направление кадра к DS (*To DS*): значение этого поля равно 1, если кадр предназначен распределительной системе или станция передает кадр другой станции через точку доступа той же BSS. Во всех остальных кадрах значение поля равно 0.

• Направление кадра от DS (*From DS*): значение этого поля равно 1, если кадр исходит из распределительной системы или точки доступа. Во всех остальных кадрах значение поля равно 0.

- Больше фрагментов (*More Fragments*): значение этого поля равно 1 во всех кадрах данных и кадрах управления, если за данным фрагментом следует несколько фрагментов, принадлежащих одному кадру. Во всех остальных кадрах значение поля равно 0.

- Повтор (*Retry*): значение поля равно 1 в любом кадре данных или кадре управления, если он является повторной передачей предыдущего. Во всех остальных кадрах значение поля равно 0. Станция-получатель использует эту информацию для исключения дублирования кадров.

- Управление мощностью (*Power management*): это поле используется для указания режима управления питанием станции после успешного завершения цикла обмена кадрами. Значение поля, равное 1, указывает, что станция будет находиться в режиме энергосбережения (*PS mode*). Значение 0 показывает, что станция будет находиться в активном режиме.

- Больше данных (*More Data*): это поле используется в кадрах данных или кадрах управления, передаваемых точкой доступа станции, находящейся в режиме энергосбережения. Значение поля, равное 1, говорит, что на точке доступа буферизировано более одного блока данных, предназначенных для этой станции.

- Защищенный кадр (*Protected Frame*): значение этого поля равно 1, если поле «Тело кадра» содержит информацию, обработанную с помощью криптографического алгоритма.

- Порядок (*Order*): значение этого поля равно 1 в двух случаях:

- а) в кадрах данных без поддержки QoS, которые должны обрабатываться с использованием строго упорядоченного класса сервиса (*Strictly Ordered service class*), т. е. строго по порядку;

- б) в кадрах данных или кадрах управления с сервисом QoS для указания, что кадр содержит поле «управление высокой пропускной способностью» (*HT Control*).

В иных случаях значение данного поля равно 0.

2.4. Управление доступом к среде в стандарте IEEE 802.11

Архитектура подуровня MAC стандарта IEEE 802.11-2012 (рис. 2.16) включает следующие функции:

- функцию распределенной координации (*Distributed Coordination Function, DCF*);

- функцию точечной координации (*Point Coordination Function, PCF*);

- функцию гибридной координации (*Hybrid Coordination Function, HCF*).

Функции DCF и PCF были определены в оригинальной спецификации IEEE 802.11-1999 для сетей, которые не поддерживают технологии качества обслуживания (QoS). Функция DCF является фундаментальным методом доступа подуровня MAC стандарта 802.11. Она реализует асинхронную передачу данных, т. е. все клиенты имеют равные возможности доступа к сети, и основывается на методе множественного доступа с контролем несущей и предотвращением коллизий (*Carrier Sense Multiple Access with Collision Avoidance*,

CSMA/CA). DCF является обязательной функцией и должна быть реализована на всех станциях для работы в IBSS и в инфраструктурном режиме.

Чтобы начать передачу, станция должна определить, свободна ли среда передачи данных, т. е. не ведется ли передача другой станцией. Если станция определяет, что среда свободна, начинается процедура передачи. В противном случае передача откладывается до окончания текущей передачи. В случае если передается одноадресный кадр, удачной считается передача, после которой получен кадр подтверждения ACK от станции-адресата. В случае многоадресной передачи — если кадр полностью передан.

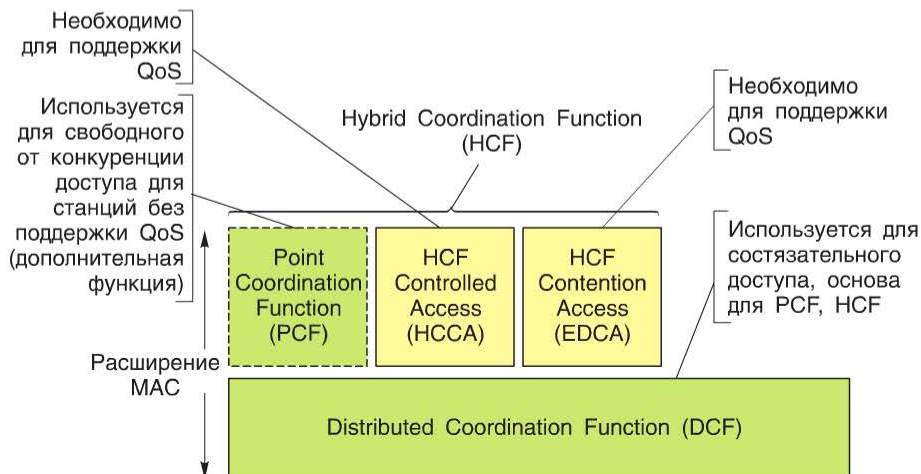


Рис. 2.16. Архитектура подуровня MAC

Для уменьшения числа коллизий может быть задействован механизм RTS/CTS: передающая и принимающая станции обмениваются контрольными кадрами *RTS (Request To Send)* и *CTS (Clear To Send)*, коллизия которых приведет к меньшим временным потерям, чем при коллизии кадров данных.

PCF является дополнительным к DCF методом доступа к среде передачи данных и применяется только в инфраструктурном режиме. Данный метод доступа использует точечный координатор (*Point Coordinator, PC*), реализованный на точке доступа в BSS. PC определяет, какая станция на текущий момент времени имеет право передавать данные. Функция PCF была разработана для передачи трафика, чувствительного к задержкам.

В результате включения в стандарт IEEE 802.11 поддержки услуг QoS появилась функция HCF, которая была определена в дополнении к стандарту IEEE 802.11e-2005. Она основана на DCF и PCF и доработана с учетом специфических механизмов QoS и подтипов кадров. HCF использует два метода доступа: соревновательный метод доступа к каналу, называемый *расширенным распределенным доступом к каналу (Enhanced Distributed Channel Access, EDCA)*, и контролируемый доступ к каналу, называемый *контролируемым HCF-доступом к каналу (HCF Controlled Channel Access, HCCA)*. DCF и централизованная функция координации (PCF или HCF) могут работать в одном BSS.

2.4.1. Функция распределенной координации (DCF)

Как уже говорилось ранее, функция DCF должна быть реализована на всех беспроводных устройствах, так как является базовым методом доступа к среде передачи. Для организации совместного доступа к среде DCF использует метод *множественного доступа с контролем несущей и предотвращением коллизий* (CSMA/CA). Протокол CSMA является хорошо известным протоколом, и его реализация CSMA/CD (*Collision Detection, CD — обнаружение коллизий*) широко используется в качестве метода доступа в сетях Ethernet. Однако метод CSMA/CD неэффективен в беспроводных сетях по причине сложной реализации механизма распознавания коллизий, поэтому в беспроводных сетях используется метод, уменьшающий вероятность их возникновения (*Collision Avoidance, CA — предотвращение коллизий*).

Механизм CSMA/CA работает следующим образом (рис. 2.17):

1) станция, желающая начать передачу, предварительно путем прослушивания беспроводной среды должна определить, занята она или свободна (т. е. выполнить *контроль несущей* частоты конкретного канала). Если среда занята, то станция откладывает передачу до ее освобождения. Как только станция фиксирует освобождение среды, она обязана отсчитать интервал времени, равный межкадровому интервалу. Если после истечения этого периода среда все еще свободна, станция запускает *таймер обратного отсчета (Backoff Timer)* с произвольно выбранным интервалом отсрочки (так называемая *процедура обратного отсчета (Backoff Procedure)*). Таймер обратного отсчета представляет собой временной интервал, разбитый на слоты фиксированной длительности. Станция проверяет состояние среды (занята или свободна) в течение каждого временного слота. Если в период времени, определенного длительностью слота, среда свободна, значение таймера обратного отсчета уменьшается на длительность одного временного слота. Если среда окажется занятой, таймер



Рис. 2.17. Блок-схема работы функции DCF

приостанавливается и начнет уменьшаться только после того, как среда будет свободной в течение периода времени, равного межкадровому интервалу. Как только длительность таймера отсрочки станет равной 0, станция начинает передачу;

2) при успешном получении кадра станция назначения посылает станции-отправителю кадр подтверждения приема (ACK). Не получив в течение определенного времени кадр ACK, станция-отправитель считает, что произошла коллизия и инициализирует процедуру повторной передачи кадра.

Контроль несущей

Функция контроля несущей в DCF осуществляется двумя параллельными механизмами: *физическим* и *виртуальным*.

Физическое обнаружение несущей выполняется на беспроводном интерфейсе устройства (на физическом уровне) и определяет активность других пользователей канала путем измерения мощности сигнала от других станций. Другими словами, выполняется измерение энергии сигнала на антенне. В результате измеренное значение сравнивается с заданным, и станция определяет, ведется ли в данный момент передача другой станцией. Физический механизм признает среду свободной, если уровень энергии сигнала на антенне не превышает заданного значения.

Виртуальный механизм контроля несущей выполняется MAC-подуровнем и основан на распространении по сети информации о длительности резервирования среды. Поле «Длительность» содержится в заголовках кадров данных, а также контрольных кадров RTS/CTS и определяет период времени, на который среда будет зарезервирована для передачи кадра (или группы кадров) и получения подтверждения приема. Устройства сети получают информацию о продолжительности текущей передачи и могут определить, сколько времени канал будет занят. Выполняется это с помощью *вектора сетевого распределения (NAV, Network Allocation Vector)*. Каждая станция, которая слышит передатчик, устанавливает свой вектор NAV (если он уже установлен, то NAV должен быть обновлен в том случае, если длительность, указанная в кадре, больше текущего значения NAV).

Для простоты NAV можно рассматривать как таймер, значения которого уменьшаются до 0 с постоянной скоростью. Он показывает, сколько времени осталось до окончания текущей передачи. Когда значение, которое показывает таймер, станет равным нулю, предполагается, что канал свободен и станция может начать состязание за доступ к среде. В противном случае считается, что канал занят и станция не может начать передачу. Другими словами, виртуальный механизм признает среду свободной при достижении вектором NAV значения 0.

Каждый из механизмов предоставляет станции информацию о состоянии среды: занята/свободна (busy/idle). Для признания среды свободной необходимо подтверждение от обоих механизмов.

Межкадровые интервалы (IFS)

Для того чтобы определить состояние беспроводной среды передачи, станция использует функцию контроля несущей в течение указанного *межкадрового интервала (Inter Frame Space, IFS)*. Межкадровый интервал определяет временной интервал между передачей кадров. В стандарте IEEE 802.11-2012 определено шесть межкадровых интервалов, которые служат для обеспечения приоритетного доступа к среде передачи (указаны в порядке увеличения длительности):

- уменьшенный межкадровый интервал (Reduced IFS, RIFS);
- короткий межкадровый интервал (Short IFS, SIFS);
- межкадровый интервал функции PCF (PCF IFS, PIFS);
- межкадровый интервал функции DCF (DCF IFS, DIFS);
- арбитражный межкадровый интервал (Arbitration IFS, AIFS);
- расширенный межкадровый интервал (Extended IFS, EIFS).

Межкадровые интервалы (IFS) независимы от скорости передачи и определяются отдельно для каждой спецификации физического уровня.

Межкадровый интервал SIFS используется, когда беспроводная станция захватила среду и ей требуется сохранить доступ к ней на время, необходимое для передачи последовательности кадров. Использование SIFS между передачей кадров позволяет предотвратить попытки захвата среды другими станциями. В некоторых случаях для уменьшения накладных расходов вместо SIFS может использоваться межкадровый интервал RIFS.

Интервал PIFS используется *точечным координатором (Point Coordinator)* функции PCF и *гибридным координатором (Hybrid Coordinator)* функции HCF для получения приоритетного доступа к среде.

Интервал DIFS используется беспроводными станциями, работающими под управлением DCF, для передачи кадров данных и управляющих кадров.

Интервал AIFS используется беспроводными станциями, поддерживающими QoS, для получения доступа к среде с помощью метода EDCA.

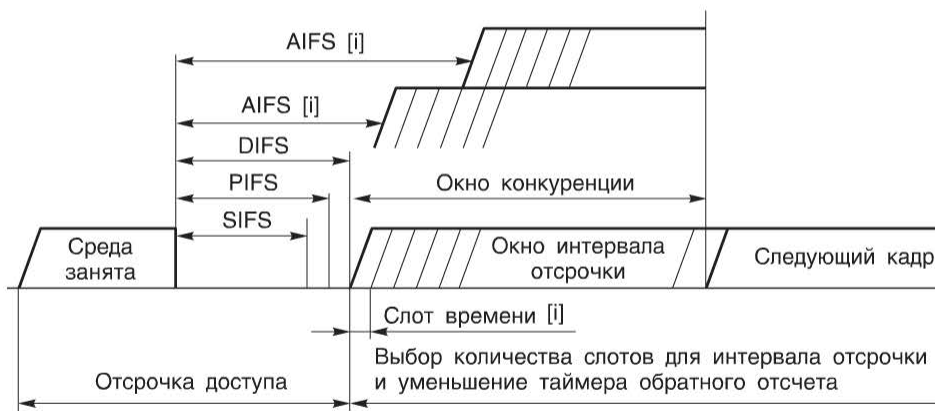


Рис. 2.18. Таймеры IFS

Интервал EIFS является самым длинным из межкадровых интервалов. Он используется функцией DCF вместо DIFS в том случае, когда станция определила, что последний полученный кадр содержал ошибку или его контрольная сумма была некорректна. После успешного получения кадра функция DCF снова переключается на использование интервала DIFS.

Значения IFS зависят от среды передачи и фиксированы (за исключением AIFS) для каждого физического уровня независимо от битовой скорости беспроводной станции.

Все временные интервалы начинают отсчитываться от момента окончания передачи очередного кадра. Это не требует передачи каких-либо специальных синхронизирующих сигналов и не ограничивает размер кадра размером временного слота, так как слоты принимаются во внимание только при принятии решения о начале передачи кадра (рис. 2.18).

Процедура обратного отсчета

Станция, желающая начать передачу кадра, должна определить состояние беспроводной среды с помощью функции контроля несущей. Если среда занята, она откладывает передачу. Если среда свободна, станция обязана отсчитать интервал времени, равный межкадровому интервалу DIFS, если последний кадр был принят ею успешно, или EIFS, если кадр был принят с ошибкой. Если после истечения периода DIFS или EIFS среда все еще свободна, станция инициирует *процедуру обратного отсчета* (*Backoff Procedure*).

Процедура обратного отсчета начинается с того, что станция должна установить *таймер обратного отсчета* (*Backoff Timer*) с произвольно выбранным интервалом отсрочки. Время отсрочки разбито на слоты фиксированной длительности и вычисляется по формуле

$$\text{Backoff Time} = \text{Random}() \cdot \text{aSlotTime},$$

где $\text{Random}()$ — псевдослучайное целое число, равномерно распределенное в интервале $[0, CW]$; *окно конкуренции* (CW , *Contention Window*) — целое число внутри диапазона значений данного физического уровня CW_{\min} и CW_{\max} ($CW_{\min} \leq CW \leq CW_{\max}$); aSlotTime — временной отрезок фиксированной длительности (временной слот), значение которого зависит от физического уровня.

Отсчет временных слотов интервала отсрочки начинается сразу после окончания периода DIFS или EIFS. Станция проверяет состояние среды (занята или свободна) в течение каждого временного слота: если среда остается свободной, значение таймера обратного отсчета уменьшается на aSlotTime . Если среда окажется занятой, процедура обратного отсчета приостанавливается, т. е. значение таймера не уменьшается. В этом случае станция начинает новый цикл доступа к среде: слежение за средой, при ее освобождении — выдерживание паузы в течение межкадрового интервала DIFS или EIFS. Если по окончании периода DIFS или EIFS среда осталась свободной, то станция возобновляет процедуру обратного отсчета и продолжает уменьшать значение таймера. Как только значение таймера обратного отсчета станет равным нулю, станция начнет передачу кадра (рис. 2.19).

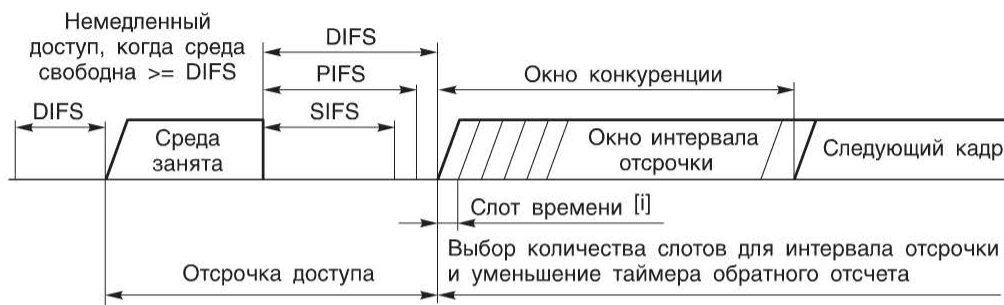


Рис. 2.19. Базовый метод доступа DCF

Процедура обратного отсчета минимизирует вероятность возникновения коллизий, когда две или более станции пытаются одновременно получить доступ к среде. Станция, выбравшая наименьший интервал отсрочки с помощью псевдослучайной функции, выигрывает соревнование за доступ к среде. Вероятность того, что две или более станции выберут один и тот же интервал отсрочки, довольно мала.

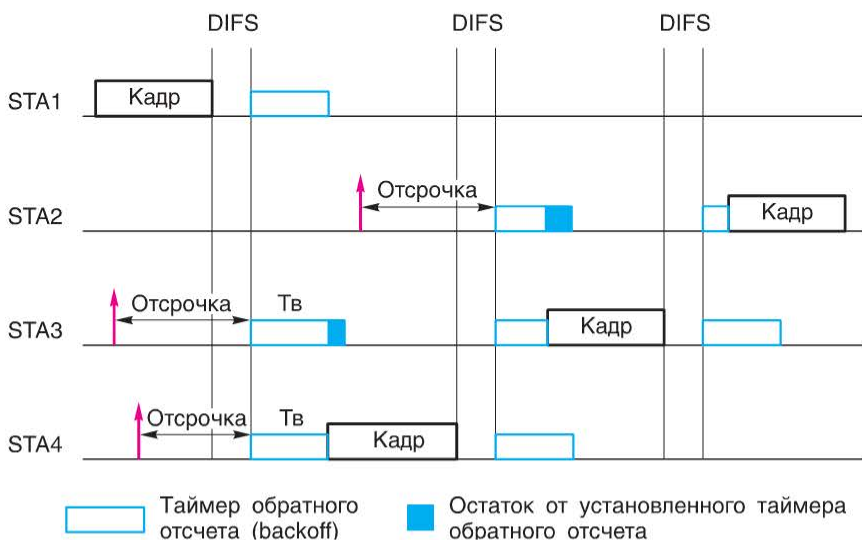


Рис. 2.20. Процедура обратного отсчета

Рассмотрим пример, показанный на рис. 2.20. Четыре станции соревнуются за доступ к среде передачи. Во время передачи кадра станцией STA1 две другие станции — STA3 и STA4 — готовы начать передачу (показаны стрелкой вверх). Обе станции откладывают начало передачи до окончания передачи кадра станцией STA1. При освобождении среды STA3 и STA4 ожидают период времени, равный DIFS, и запускают свои таймеры обратного отсчета, вычисленные случайным образом. Таймер станции STA4 достигнет

нуля раньше, и она начинает передачу. Станция STA3 при этом остановит свой таймер. Во время передачи кадром станцией STA4 станция STA2 переходит к готовности передачи очередного кадра. Таким образом, после завершения станцией STA4 передачи кадра и истечения периода DIFS станции STA2 и STA3 будут соревноваться за доступ к среде. STA3 продолжит уменьшение значения своего таймера обратного отсчета, а STA2 запустит таймер с произвольно выбранным значением. Таймер обратного отсчета STA3 достигнет нуля быстрее, поэтому STA3 начнет передачу. После завершения передачи станцией STA3 и окончания периода DIFS STA2 продолжит уменьшать свой таймер обратного отсчета и начнет передачу сразу, как только он станет равным нулю.

Подтверждение приема кадра

Для подтверждения факта успешного получения каждого переданного кадра данных используются *мгновенные подтверждения (квитанции)*. Кадр подтверждения приема (ACK) (рис. 2.21) должен быть передан станцией назначения сразу после успешного получения одноадресного кадра данных через временной интервал SIFS, невзирая на состояние среды передачи (рис. 2.22).



Рис. 2.21. Формат кадра ACK

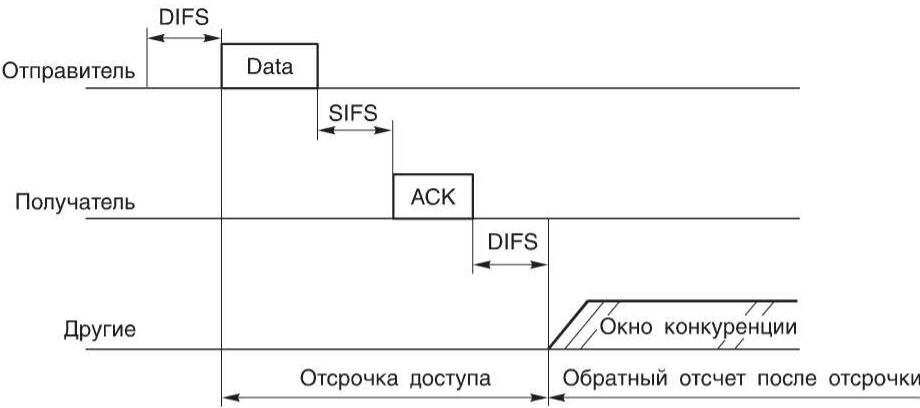


Рис. 2.22. Передача кадра ACK

Не получив подтверждения в течение определенного времени, станция-отправитель считает, что произошла ошибка, и инициирует процедуру повторной передачи кадра. При этом время обратного отсчета будет вычисляться с использованием нового значения окна конкуренции при каждой повторной передаче.

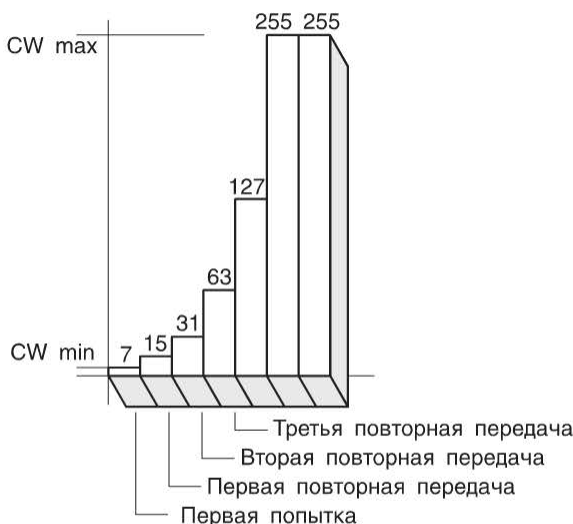


Рис. 2.23. Экспоненциальное увеличение CW

Первоначальное значение окна конкуренции равно CW_{min} . Оно экспоненциально возрастает при каждой неудачной попытке передачи кадра до тех пор, пока не достигнет CW_{max} . Как только CW достигнет CW_{max} , оно остановится на этом значении до успешной передачи кадра или до истечения лимита повторных передач (рис. 2.23). При успешной передаче кадра CW сбрасывается до значения CW_{min} . Эта процедура позволяет уменьшить вероятность коллизий и повысить стабильность метода доступа в условиях высокой загрузки сети.

Следует сказать об ограничениях реализации QoS в DCF. Чувствительные к задержкам приложения, такие, как сетевые игры, VoIP, видеоконференции и др., требуют гарантированной полосы пропускания, задержки передачи, потерь пакетов. Функция DCF обеспечивает только *негарантированную доставку данных (Best Effort Service)*, т. е. не предполагает проведения какой-либо классификации трафика. Это ограничение DCF устраняется методом доступа EDCA.

Проблема скрытого узла

Следует учитывать, что в беспроводных сетях не все станции могут находиться в зоне действия друг друга, что приводит к различным проблемам. В частности, каждая станция, использующая метод CSMA/CA, пытается избежать коллизий путем определения уровня сигнала на передатчике. Однако коллизии возникают в приемнике, когда два и более сигнала создают помехи друг другу. Поскольку приемник и передатчик разнесены, механизм обнаружения коллизий не предоставляет достаточно информации для избежания коллизии. Чтобы лучше понять эту проблему, рассмотрим пример

с тремя беспроводными станциями (рис. 2.24), причем станции А и В не находятся в зоне действия друг друга.

Предположим, что станция А и станция В начали одновременно передавать данные станции С, в зоне действия которой они находятся. Когда станция А начинает передачу, она не слышит станцию В, так как последняя находится вне зоны ее действия, и наоборот. В результате сигналы от этих станций будут создавать помехи друг другу. Такая ситуация называется *проблемой скрытого узла (hidden station)* — станция не может определить потенциального соперника за полосу пропускания, поскольку соперник находится вне зоны ее действия.

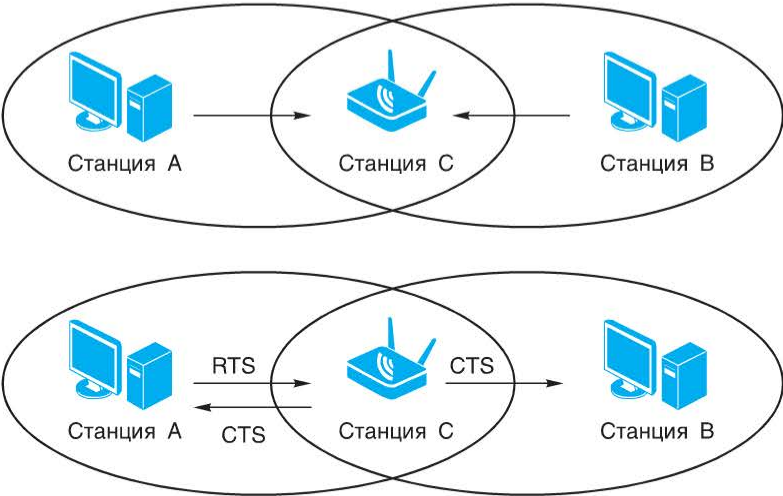


Рис. 2.24. Проблема скрытого узла и ее решение

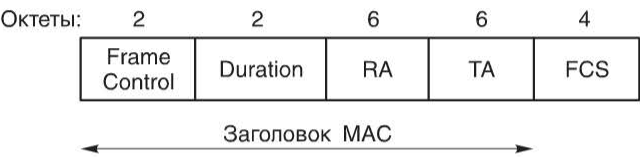


Рис. 2.25. Формат кадра RTS

Для преодоления этой проблемы в стандарте IEEE 802.11 используются контрольные кадры RTS/CTS. Механизм RTS/CTS является расширением метода доступа DCF. Станция, собирающаяся передать данные, инициализирует процесс отправкой кадра RTS (*Request To Send, запрос на передачу*) (рис. 2.25). На этот запрос станция назначения должна ответить служебным кадром CTS (*Clear To Send, свободна для передачи*) (рис. 2.26).

Правила передачи кадров RTS точно такие же, как при передаче кадров данных. Передатчик отправляет кадр RTS после того, как среда будет сво-

бодна в течение временного интервала DIFS (рис. 2.27). Каждая станция, принимающая RTS, читает поле «Длительность» кадра и устанавливает свой вектор сетевого распределения (NAV), определяющий период времени, на который она должна воздержаться от доступа к среде. После получения кадра RTS станция назначения отвечает кадром CTS через интервал SIFS. Станции, получающие кадр CTS, читают его поле «Длительность» (его значение аналогично значению поля в кадре RTS) и обновляют свои векторы NAV. Успешный обмен кадрами RTS/CTS позволяет зарезервировать канал на время, требуемое станции-отправителю для передачи кадра данных. При успешном получении кадра CTS станция-отправитель выжидает интервал SIFS и посылает кадр данных. Если кадр CTS не был получен, повторная отправка кадра RTS последует только после выполнения процедуры обратного отсчета.

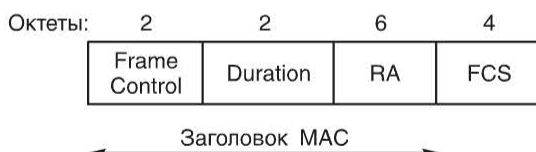


Рис. 2.26. Формат кадра CTS

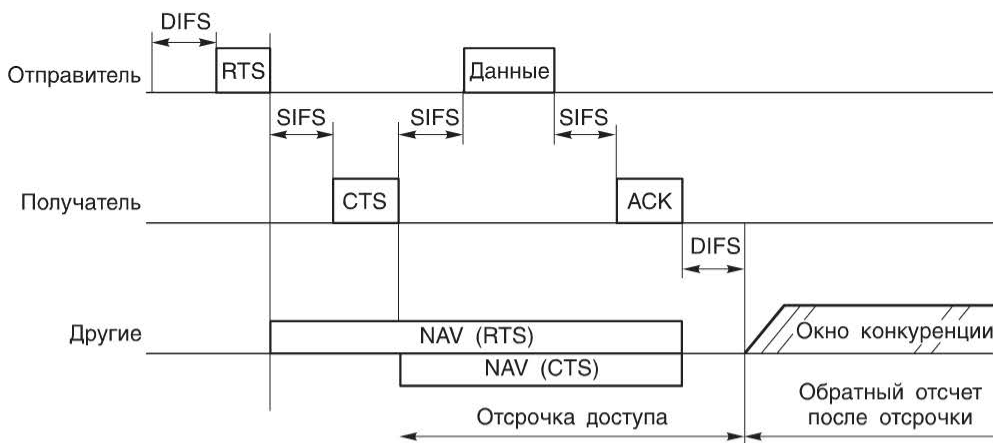


Рис. 2.27. Доступ к среде передачи с помощью кадров RTS/CTS

Размер управляющих кадров RTS и CTS относительно небольшой по сравнению с размером кадра данных: длина кадра RTS — 20 байт, кадра CTS — 14 байт. Так как кадры RTS и CTS гораздо короче, чем кадр данных, то потери данных в результате коллизии кадров RTS или CTS гораздо меньше, чем при коллизии кадров данных.

Механизм RTS/CTS не может использоваться для передачи широковещательных или многоадресных кадров, так как в этом случае существует несколько потенциальных отправителей CTS. Процедура обмена кадрами

RTS и CTS в этом случае не обязательна. От нее можно отказаться, если в сети нет скрытых узлов, а также при небольшой нагрузке сети, поскольку в такой ситуации коллизии случаются редко, а значит, не стоит тратить дополнительное время на выполнение процедуры обмена кадрами RTS и CTS.

2.4.2. Функция точечной координации (PCF)

Функция PCF является дополнительным к DCF методом доступа, который применяется только в инфраструктурном режиме. Данный метод доступа основан на процедуре опроса и использует *точечный координатор (Point Coordinator, PC)*, реализованный на точке доступа, который исполняет роль мастера опроса. PC определяет, какая станция на текущий момент времени имеет право передавать данные, т. е. управляет коллективным доступом к среде передачи. PCF использует виртуальный механизм контроля несущей, опирающийся на механизм приоритетного доступа.

PCF является необязательным методом доступа. Для того чтобы использовать его в сети, он должен поддерживаться точкой доступа и станциями. Функции PCF и DCF могут одновременно работать в одной сети. При работающем точечном координаторе методы доступа PCF и DCF сменяют друг друга. Время, когда точка доступа работает в режиме PCF, называется *свободный от конкуренции период (Contention-Free Period, CFP)*. В течение этого периода точка доступа опрашивает станции, поддерживающие функцию PCF, об их намерении передавать данные и на основании этого опроса организует обмен кадрами между узлами сети. Такой подход полностью исключает состязательный доступ к среде (как в случае метода DCF) и делает невозможным возникновение коллизий, а для чувствительных к задержкам приложений гарантирует приоритетный доступ к среде. Таким образом, PCF может использоваться для организации приоритетного доступа к среде передачи данных.

Время, когда точка доступа работает в режиме DCF, называется *период конкуренции (Contention Period, CP)*. Станции сети, которые не сконфигурированы для упорядоченного опроса, будут состязаться за доступ к среде с использованием метода CSMA/CA.

Основные термины PCF

Функция точечной координации (Point Coordination Function, PCF) — класс функций координации, при которых логика функции координации активна только на одной станции базового набора услуг (BSS) в любой момент времени использования сети.

Точечный координатор (Point Coordinator, PC) — объект станции, являющейся точкой доступа, который выполняет функцию точечной координации.

Свободный от конкуренции период (Contention-Free Period, CFP) — период времени, в течение которого выполняется функция точечной координации (PCF), когда право на передачу предоставляется станции исключительно точечным координатором (PC), позволяющим обмениваться данными членам базового набора услуг (BSS) без состязания за доступ к беспроводной среде.

Период конкуренции (*Contention Period, CP*) — период времени за пределами свободного от конкуренции периода (CFP) в базовом наборе услуг (BSS) с точечной функцией координации. В BSS без точечного координатора (PC) период конкуренции является временем работы BSS.

Для возможности чередовать режимы PCF и DCF (рис. 2.28) необходимо, чтобы точка доступа, выполняющая функцию точечного координатора и реализующая режим PCF, имела приоритетный доступ к среде передачи данных. Это можно сделать, если использовать соревновательный доступ к среде передачи данных, но с меньшими, чем в режиме DCF, межкадровыми интервалами. В начале свободного от конкуренции периода точечный координатор должен убедиться, что среда не занята и первым получить доступ к ней. Для этого он использует промежуток ожидания PIFS, который меньше DIFS. Если по истечении периода времени, определенного PIFS, среда свободна, точечный координатор отправляет сигнальный кадр (*Beacon Frame*), информирующий станции, что начался свободный от конкуренции период (CFP), и сообщает его длительность. Получив сигнальный кадр, все станции сети устанавливают свои векторы NAV равными продолжительности CFP. Эти действия позволяют точечному координатору получить контроль над средой передачи и удерживать его в течение всего периода, свободного от конкуренции. Период CFP должен повторяться с определенной периодичностью и синхронизироваться с интервалом передачи сигнальных кадров (*Beacon Interval*). При этом для того, чтобы какая-то доля среды всегда доставалась асинхронному трафику, длительность свободного от конкуренции периода ограничена.

После передачи сигнального кадра точечный координатор ожидает интервал времени, равный SIFS, и затем начинает передачу одного из следующих кадров: кадра данных (Data), кадра CF-опрос (CF-Poll), кадра данные + CF-опрос (Data+CF-Poll), кадра управления или кадра CF-окончание (CF-End).

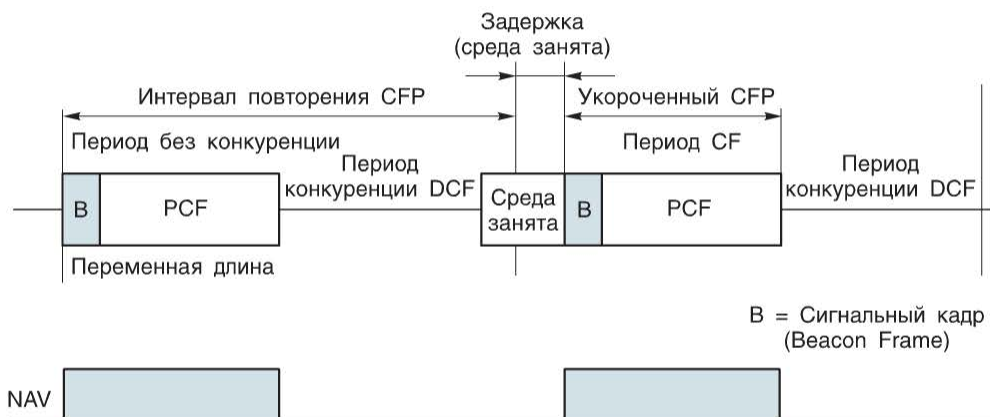


Рис. 2.28. Чередование периодов CFP и CP

Точечный координатор выполняет процедуру упорядоченного опроса всех станций, сконфигурированных для работы в РСF, чтобы по очереди предоставить каждой из них право на использование среды. Для этого он последовательно отправляет специальный кадр CF-опрос (CF-Poll) станциям, включенным в его опросный лист. Опрашиваемые станции в ответ на получение кадров CF-опрос посылают кадр CF-подтверждение (CF-Ack). Если подтверждения не получено, то точечный координатор переходит к опросу следующей станции.

Чтобы иметь возможность организовать передачу данных между всеми узлами сети, точка доступа может передавать кадр данных (Data) и совмещать кадр опроса с передачей данных (кадр Data+CF-Poll). Аналогично станции могут совмещать кадры подтверждения с передачей данных, передавая кадры Data+CF-Ack (рис. 2.29).

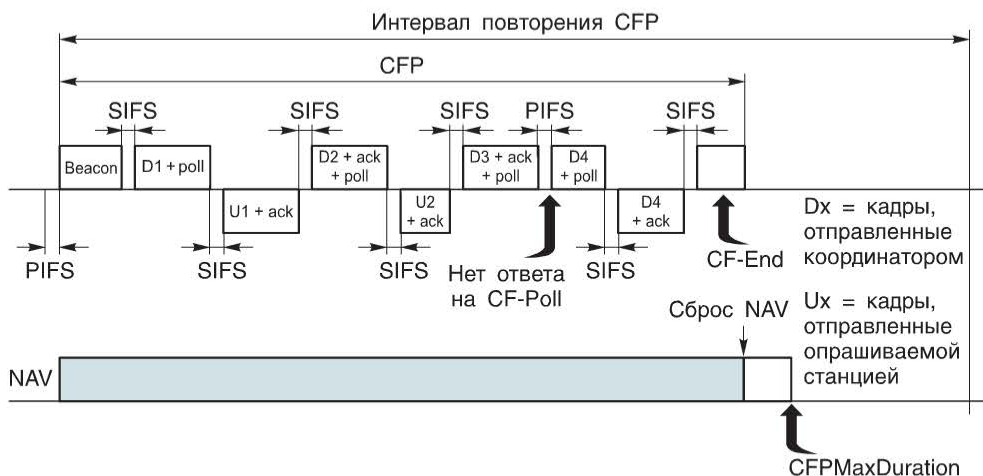


Рис. 2.29. Пример передачи кадров в режиме PCF

В конце каждого периода CFP точечный координатор передает кадр CF-окончание (CF-End) или CF-окончание+подтверждение (CF-End+CF-Ack), сообщая, что контролируемый период закончился и начинается период конкуренции. Кадр CF-окончание также может быть передан до истечения периода CFP в том случае, если у станций, сконфигурированных для упорядоченного опроса, нет данных для передачи. После получения такого кадра все станции должны сбросить значение NAV.

2.4.3. Понятие QoS

При передаче по единой сети трафика потоковых мультимедийных приложений (Voice over IP (VoIP), IPTV, видеоконференции, он-лайн игры и др.) и трафика данных с различными требованиями к пропускной способности необходимы механизмы, обеспечивающие возможность дифференцирования

и обработки различных типов сетевого трафика в зависимости от предъявляемых ими требований. Негарантированная доставка данных (*best effort service*), традиционно используемая в сетях, не предполагает проведения какой-либо классификации трафика и не обеспечивает надежной доставки трафика приложений, гарантированную пропускную способность канала и определенный уровень потери пакетов. Для решения этой проблемы было введено понятие *качества обслуживания (Quality of Service, QoS)*.

Функции качества обслуживания в современных сетях заключаются в обеспечении гарантированного и дифференцированного уровня обслуживания сетевого трафика, запрашиваемого теми или иными приложениями на основе различных механизмов распределения ресурсов, ограничения интенсивности трафика, обработки очередей и приоритизации. Можно выделить три модели реализации QoS в сетях:

- негарантированная доставка данных (*Best Effort Service*) — обеспечивает связь между узлами, но не гарантирует надежную доставку данных, время доставки, пропускную способность и определенный приоритет;
- интегрированные услуги (*Integrated Services, IntServ*) — эта модель описана в RFC 1633 и предполагает предварительное резервирование сетевых ресурсов с целью обеспечения предсказуемого поведения сети для приложений, требующих для нормального функционирования гарантированной выделенной полосы пропускания на всем пути следования трафика. Эту модель также часто называют *жестким QoS (hard QoS)* в связи с предъявлением строгих требований к ресурсам сети;
- дифференцированное обслуживание (*Differentiated Service, DiffServ*) — эта модель описана в RFC 2474, RFC 2475 и предполагает разделение трафика на классы на основе требований к качеству обслуживания. В архитектуре DiffServ каждый передаваемый пакет снабжается информацией, на основании которой принимается решение о его продвижении на каждом промежуточном узле сети в соответствии с политикой обслуживания трафика данного класса (*Per-Hop Behavior, PHB*). Модель дифференцированного обслуживания занимает промежуточное положение между негарантированной доставкой данных и моделью IntServ и сама по себе не предполагает обеспечение гарантий предоставляемых услуг, поэтому дифференцированное обслуживание часто называют *мягким QoS (soft QoS)*.

2.4.4. Функция гибридной координации (HCF)

Изначально определенные в стандарте IEEE 802.11 методы доступа DCF и PCF не обеспечивают возможностей качества обслуживания. Метод DCF основан на конкуренции станций за доступ к среде передачи. Метод PCF обеспечивает приоритетный доступ станций к среде передачи, но не позволяет выполнять дифференцированную обработку трафика разных приложений. В связи с этим в 2005 году появилось дополнение к стандарту IEEE 802.11, получившее название IEEE 802.11e-2005 или IEEE 802.11e. В этом дополнении определен набор функций для обеспечения качества обслужи-

вания в беспроводных сетях. Позднее оно стало частью стандарта IEEE 802.11-2007. Таким образом, подуровень MAC стандарта IEEE 802.11 был дополнен функцией гибридной координации (HCF).

Функция HCF основана на DCF и PCF и доработана с учетом специфических механизмов QoS и подтипов кадров. Она поддерживает передачу кадров между станциями в период конкуренции (CP) и свободный от конкуренции период (CFP). Для этого HCF использует два метода доступа: соревновательный метод доступа к каналу, называемый *расширенным распределенным доступом к каналу* (*Enhanced Distributed Channel Access, EDCA*) и контролируемый доступ к каналу, называемый *контролируемым HCF-доступом к каналу* (*HCF Controlled Channel Access, HCCA*).

Основные определения HCF

Гибридная функция координации (*Hybrid Coordination Function, HCF*) — функция координации, которая комбинирует и улучшает методы доступа с конкуренцией и с отсутствием конкуренции, обеспечивая станциям с поддержкой качества обслуживания (QoS) приоритетный и параметризованный доступ к беспроводной среде передачи, поддерживая при этом передачу трафика станций без поддержки QoS (*best-effort*).

Возможность передачи (*Transmission Opportunity, TXOP*) — интервал времени, в течение которого определенная станция с поддержкой качества обслуживания (QoS) получает право начать передачу последовательности кадров через беспроводную среду. TXOP определяется начальным временем и максимальной продолжительностью. TXOP может быть получен станцией либо после успешного состязания за канал, либо после назначения гибридным координатором (HC).

Гибридный координатор (*Hybrid Coordinator, HC*) — тип координатора, являющегося частью устройства с поддержкой качества обслуживания (QoS), который выполняет обмен последовательностями кадров и правила обработки MSDU, определенные функцией гибридной координации (HCF). Гибридный координатор функционирует как в период конкуренции (CP), так и в свободный от конкуренции период (CFP). HC выполняет управление полосой пропускания, включая выделение возможностей передачи (TXOP) станциям с поддержкой QoS. HC функционирует на точке доступа с поддержкой QoS.

Функция HCF обеспечивает станции возможность передать за один раз сразу несколько кадров. Когда станция получает доступ к среде передачи, ей выделяется определенный период времени (*возможность передачи, TXOP*), в течение которого она может передавать данные.

Расширенный распределенный доступ к каналу (EDCA)

Расширенный распределенный доступ к каналу (EDCA) — это метод доступа, обеспечивающий дифференцированный, распределенный доступ станций к беспроводной среде передачи, используя восемь уровней приоритетов пользователей (*user priority, UP*), которые привязаны к четырем категориям доступа (*access categories, AC*) для доставки трафика. Эти категории доступа

(background (AK_BK), best effort (AK_BE), video (AK_VI), voice (AK_VO)) определяют способ обработки кадров.

Для обеспечения QoS на канальном уровне кадр 802.11 содержит поле QoS Control, включающее подполе TID (*Traffic Indicator*, *индикатор трафика*) длиной 3 бита, которое позволяет задать приоритет кадра. Всего существует восемь приоритетов пользователя: от 0 до 7, где 7 — наивысший (табл. 2.2). Эти приоритеты аналогичны приоритетам пользователя, определенным в стандарте IEEE 802.1D, благодаря чему можно обеспечивать требуемый уровень обслуживания кадров при их передаче как по проводным, так и по беспроводным сетям.

Таблица 2.2. Привязка приоритетов к категориям доступа

Приоритет	Приоритет пользователя (аналогичен 802.1D)	Категория доступа
<div style="display: flex; align-items: center; justify-content: center;"> <div style="text-align: center; margin-right: 10px;"> ↓ </div> <div style="text-align: center;"> Низкий Самый высокий </div> </div>	1	AC_BK
	2	AC_BK
	0	AC_BE
	3	AC_BE
	4	AC_VI
	5	AC_VI
	6	AC_VO
	7	AC_VO

На беспроводном устройстве, реализующем QoS, поддерживается четыре независимые очереди передачи — по одной для каждой категории доступа. Для того чтобы поместить кадр в одну из очередей, устройство анализирует данные о приоритете в поле QoS Control (рис. 2.30) и затем в соответствии с картой привязки приоритетов к категориям доступа направляет кадр в соответствующую очередь. Этот процесс называется классификацией.

Каждая категория доступа (очередь) соревнуется за возможность передачи (TXOP), т. е. за получение доступа к среде передачи данных. Для этого используется расширенный вариант DCF, называемый *расширенной функцией распределенного доступа к каналу* (*Enhanced Distributed Channel Access Function*, *EDCAF*). Параметры доступа (межкадровые интервалы, значения CW_{\min} и CW_{\max}) к каналу связи разные для каждой категории доступа. Кадры из высокоприоритетной категории доступа имеют большую вероятность получить возможность передачи (TXOP) в процессе состязания за среду передачи (рис. 2.31). Если кадры из разных категорий доступа (очередей) создают внутреннюю коллизию, то первым будет передан кадр с наивысшим приоритетом, а для кадра с меньшим приоритетом изменится значение таймера обратного отсчета так же, как это делается при возникновении внешней коллизии.

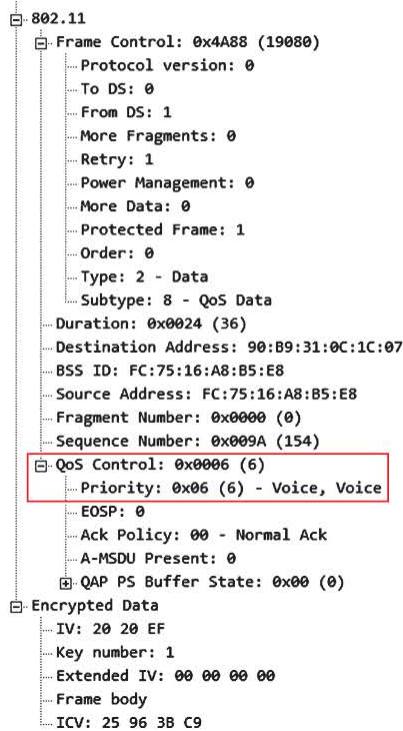


Рис. 2.30. Кадр данных с информацией о приоритете

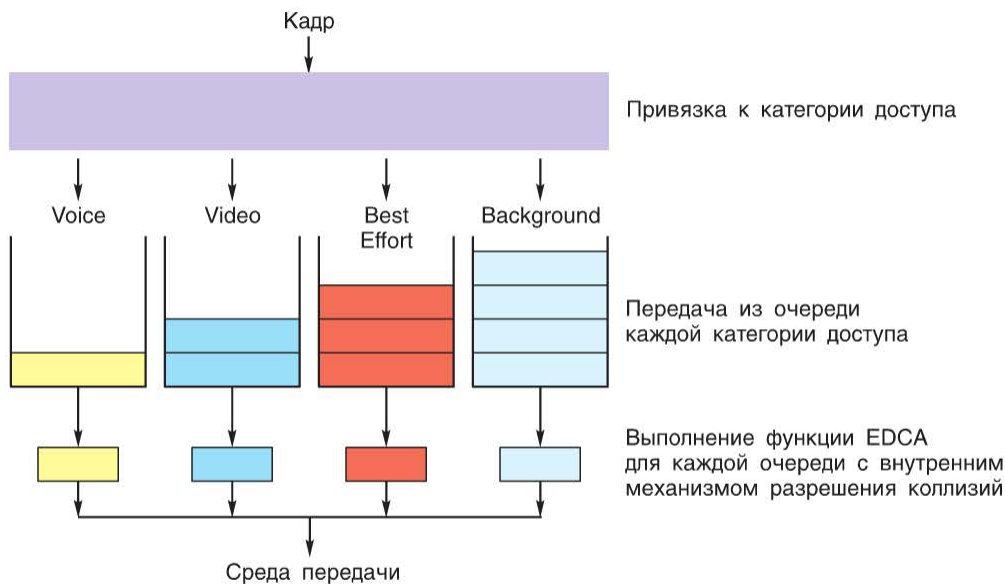


Рис. 2.31. Очереди беспроводного устройства с поддержкой QoS

Контролируемый HCF-доступ к каналу (HCCA)

Механизм HCCA использует централизованный координатор с поддержкой QoS, называемый *гибридным координатором (Hybrid Coordinator, HC)*, который работает в соответствии с правилами, отличными от точечного координатора в PCF. Гибридный координатор работает на точке доступа и имеет наивысший приоритет для доступа к беспроводной среде с целью передачи кадров. Используя высокий приоритет, он может выделять возможность передачи (TXOP) для себя и других станций, предоставляя ограниченный по времени период контролируемого доступа для передачи данных с QoS.

2.4.5. Программа сертификации Wi-Fi Multimedia (WMM)

Современные беспроводные сети значительно загружены трафиком мультимедийных приложений, чувствительных к задержкам и потерям пакетов. Wi-Fi Alliance разработал несколько сертификационных программ, которые позволяют оптимизировать производительность беспроводных сетей путем управления требованиями трафика различного типа к качеству обслуживания.

В 2004 году Wi-Fi Alliance определил требования к QoS в беспроводных сетях семейства 802.11 и представил программу сертификации Wi-Fi Multimedia (WMM), которая была основана на проекте стандарта IEEE 802.11e, ратифицированного в 2005 году. Сертификация WMM является опциональной для устройств Wi-Fi, поскольку не всем приложениям требуется QoS, но если беспроводное устройство (точка доступа или беспроводной адаптер) поддерживает функциональность QoS, для него требуется сертификация WMM. Сертификация WMM гарантирует, что беспроводные устройства с поддержкой QoS будут совместимы друг с другом и смогут взаимодействовать с беспроводными устройствами без поддержки QoS.

WMM обеспечивает классификацию трафика на основе 8 уровней приоритетов, которые привязываются к четырем категориям доступа (табл. 2.3). Последние, в свою очередь, привязываются к четырем очередям. WMM основана на методе доступа EDCA.

Таблица 2.3. Категории доступа WMM

Категории доступа WMM	Описание	Приоритет 802.1D
WMM Voice Priority	Наивысший приоритет Трафик VoIP и другой трафик, требующий минимальных задержек при передаче	7, 6
WMM Video Priority	Приоритетная передача видеотрафика по сравнению с трафиком данных	5, 4
WMM Best Effort Priority	Трафик устаревших устройств или устройств без поддержки QoS Трафик не столь чувствительный к задержкам, такой как просмотр Web-страниц	0, 3

Категории доступа WMM	Описание	Приоритет 802.1D
WMM Background Priority	Низкоприоритетный трафик, не имеющий жестких требований к задержкам и полосе пропускания, такой как загрузка файлов, сетевая печать и т. п.	2, 1

В 2005 году Wi-Fi Alliance также определил программу сертификации WMM-Power Save, которая основана на расширенном механизме сохранения энергии, определенном в IEEE 802.11e для продления срока службы батарей мобильных устройств.

В 2012 году появилась программа сертификации WMM-Admission Control, повышающая производительность беспроводных сетей при передаче голосового и видеотрафика. Для этого к приоритизации трафика с помощью категорий доступа, определенных в WMM, добавляется управление полосой пропускания канала связи.

2.4.6. Фрагментация кадров в беспроводной сети

Для того чтобы повысить надежность передачи больших блоков данных, поступающих с подуровня LLC на подуровень MAC, может потребоваться их *фрагментация (fragmentation)* — функция подуровня MAC, выполняющая дробление исходного кадра на кадры меньшего размера (фрагменты) с целью повышения надежности передачи (рис. 2.32). Предполагается, что вероятность успешной передачи фрагмента кадра через зашумленную беспроводную среду выше. Каждый фрагмент передается отдельно от остальных. Получение каждого фрагмента кадра также подтверждается отдельно, следовательно, если какой-нибудь фрагмент кадра будет передан с ошибкой или вступит в коллизию, то передавать повторно придется только его, а не весь кадр. Это увеличивает пропускную способность среды передачи информации.

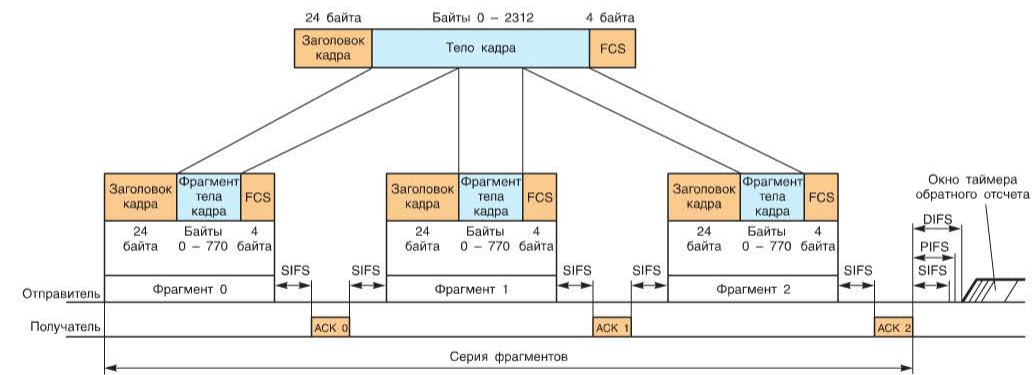


Рис. 2.32. Фрагментация кадра

Размер фрагмента может задавать администратор сети. Фрагментации подвергаются только одноадресные кадры. Широковещательные и многоадресные кадры передаются целиком.

Несмотря на то что за счет фрагментации можно повысить надежность передачи кадров в беспроводных сетях, она приводит к росту служебного трафика («накладных расходов»). Каждый фрагмент кадра снабжается отдельным заголовком, а также требует передачи соответствующего кадра подтверждения, что снижает реальную производительность беспроводной сети. Фрагментация обеспечивает баланс между надежностью и непроизводительной загрузкой беспроводной среды передачи данных. Процесс, обратный фрагментации, называется *дефрагментацией* (*defragmentation*) и выполняется на стороне приемника.

3. Подключение клиента к беспроводной сети в инфраструктурном режиме

Рассмотрим процесс подключения беспроводного клиента к беспроводной сети, работающей в инфраструктурном режиме. Для того чтобы беспроводное устройство стало полноценным членом беспроводной сети, т. е. ас-

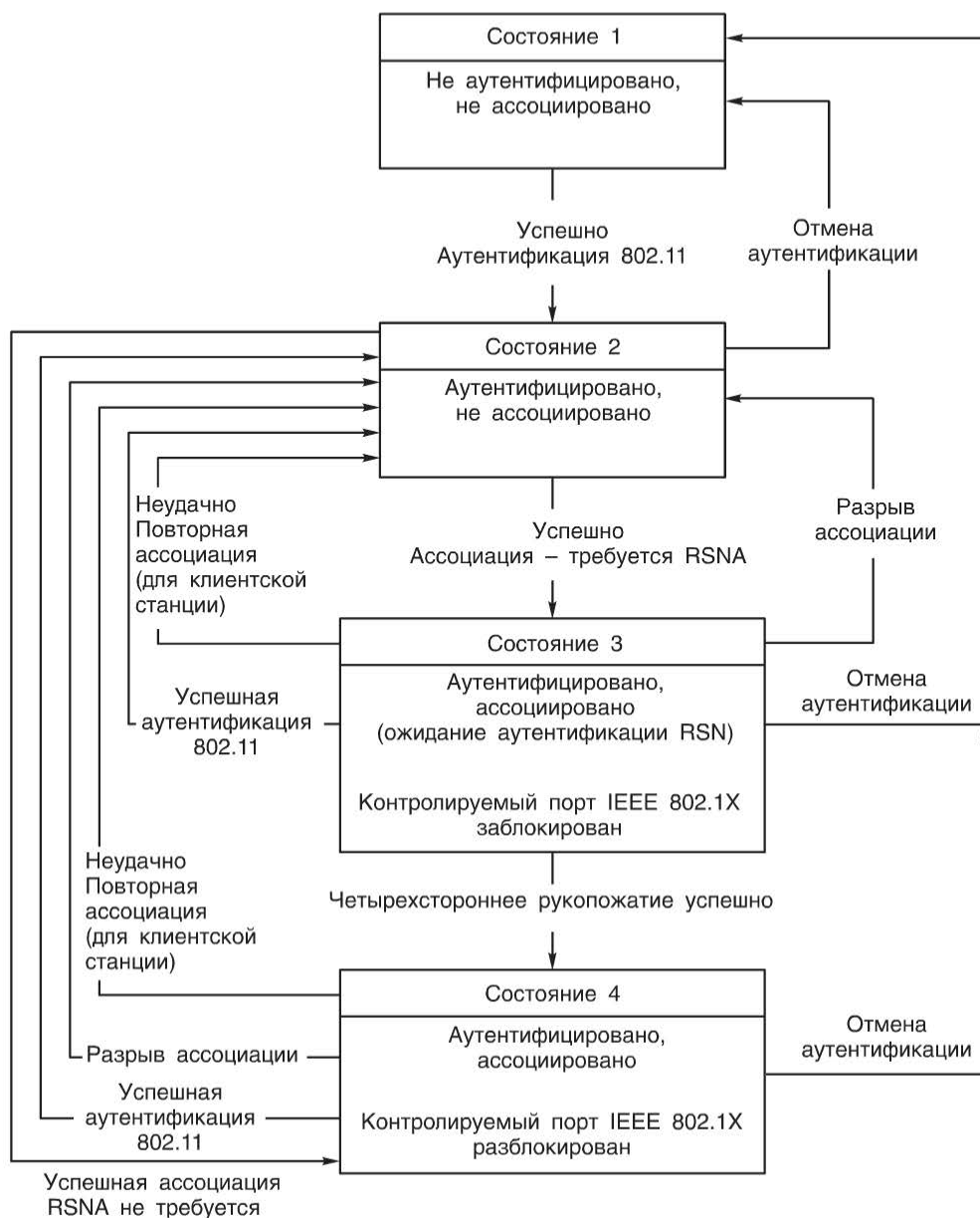


Рис. 3.1. Диаграмма состояний (машина состояний) беспроводного клиента

социировалось с точкой доступа, оно должно последовательно пройти через четыре состояния.

Состояние 1: начальное состояние, не аутентифицировано, не ассоциировано.

Состояние 2: аутентифицировано, не ассоциировано.

Состояние 3: аутентифицировано и ассоциировано (в ожидании аутентификации RSN).

Состояние 4: аутентифицировано и ассоциировано.

Диаграмма состояний показана на рис. 3.1.

Для того чтобы беспроводное устройство могло начать передачу данных через точку доступа, оно должно находиться в состоянии «аутентифицировано и ассоциировано». Переход в это состояние выполняется устройством поэтапно путем обмена последовательностями кадров управления 802.11.

Первым действием беспроводного устройства, находящегося в начальном состоянии, является обнаружение беспроводных сетей, в зоне действия которых оно находится.

3.1. Сканирование

Для работы беспроводных устройств выделены определенные частотные диапазоны. Каждый диапазон, в свою очередь, делится на *каналы (channel)*, количество и ширина которых зависят от используемой на физическом уровне 802.11 технологии и позволяющие беспроводным устройствам взаимодействовать друг с другом.

Как только точка доступа переходит в активное состояние, она начинает широковещательно отправлять через определенные временные интервалы в каждый канал *сигнальные кадры (Beacon Frame)*, содержащие информацию о функциональных возможностях точки доступа, поддерживаемых скоростях, политиках безопасности, значении SSID (рис. 3.2).

До начала работы на точке доступа и станциях, входящих в сеть, должны быть сконфигурированы все параметры, требуемые для нормального функционирования сети.

Перед подключением к точке доступа беспроводной клиент проводит активное или пассивное сканирование каждого канала с целью определения доступных сетей (точек доступа).

В ходе *пассивного сканирования* станция прослушивает каждый канал в течение определенного периода времени на предмет обнаружения передаваемых точками доступа сигнальных кадров. По содержащейся в сигнальных кадрах информации о SSID и определяются доступные для подключения беспроводные сети.

При *активном сканировании* (рис. 3.3) клиент последовательно отправляет широковещательные кадры *пробного запроса (Probe Request)* в каждый из проверяемых каналов. Кадр пробного запроса (рис. 3.4) содержит такую информацию, как поддерживаемые скорости передачи и стандарты, значение SSID.

Для того чтобы все точки доступа могли получить запрос, в качестве адреса назначения и идентификатора BSSID указывается широковещательный адрес FF:FF:FF:FF:FF:FF.

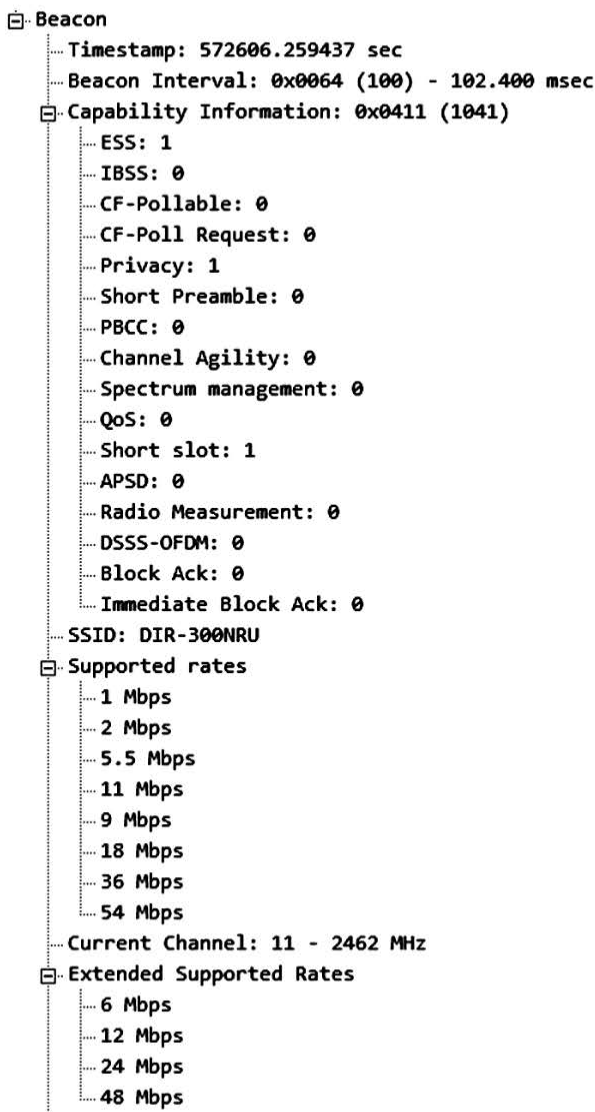


Рис. 3.2. Сигнальный кадр

3. Подключение клиента к беспроводной сети...

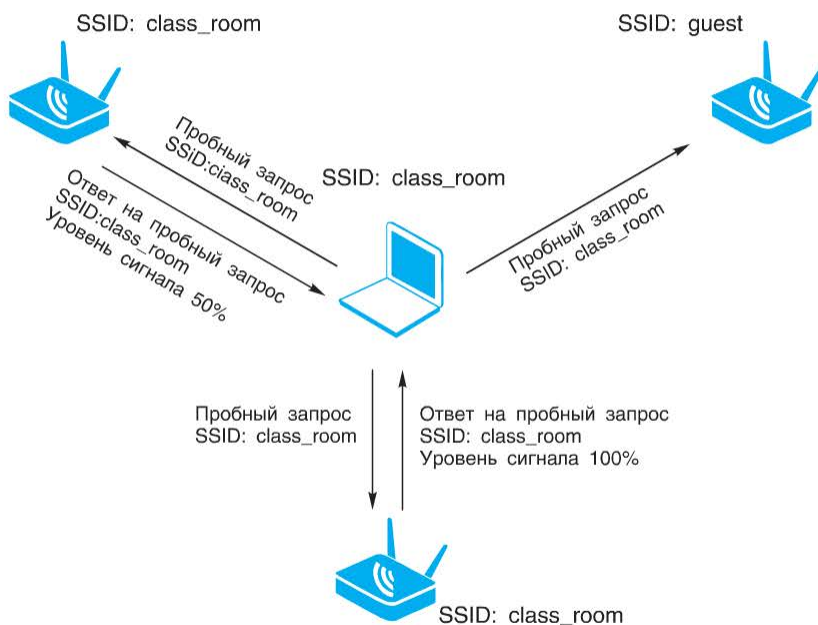


Рис. 3.3. Активное сканирование

Точка доступа отвечает на пробный запрос в том случае, если значение SSID в поступившем запросе совпадает с ее собственным либо является *Wildcard SSID* (SSID нулевой длины, означающий «все SSID»). Ответ на пробный запрос (*Probe Response*) (рис. 3.5) содержит информацию о SSID, поддерживаемых скоростях передачи, типах шифрования и других возможностях точки доступа. Он посылается на индивидуальный адрес станции, отправившей запрос.

Клиент может получить ответ на пробный запрос от нескольких точек доступа большой сети и должен выбрать, к какой из них подключиться. Механизм, по которому клиент выбирает точку доступа для ассоциации с ней, не описан в стандарте IEEE 802.11 и реализуется производителями оборудования самостоятельно.

В общем случае критерий выбора точки доступа может быть основан на SSID, уровне сигналов, совместимых типах шифрования и аутентификации, собственных критериях производителя.

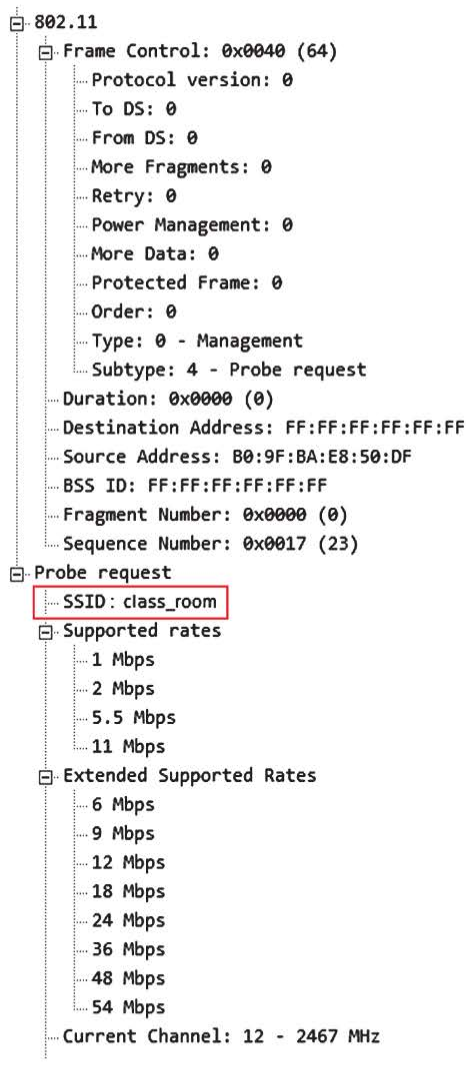


Рис. 3.4. Кадр пробного запроса

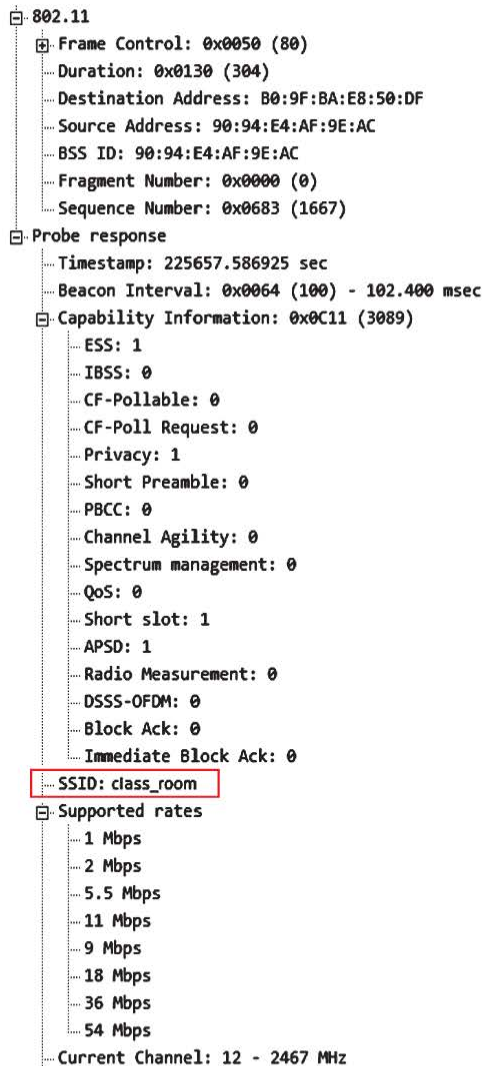


Рис. 3.5. Кадр ответа на пробный запрос

3.2. Аутентификация и ассоциация

Перед началом работы в сети на точках доступа и станциях должны быть настроены функции безопасности: выбраны криптографические алгоритмы, алгоритмы распределения ключей, методы аутентификации и т. д. Станция узнает о функциях безопасности, в том числе методах аутентификации, поддерживаемых точкой доступа из полученных от нее кадров Beacon или Probe Response (рис. 3.6). После того как станция выбрала точку доступа для подключения, она отправляет ей запрос на аутентификацию. В сетях IEEE 802.11 может использоваться один из следующих типов аутентификации:

- открытых систем (*Open System authentication*);
- с общим ключом (*Shared Key authentication*);
- при быстром переходе BSS (*FT authentication*);
- с использованием пароля (*Simultaneous Authentication of Equals, SAE*);
- на основе стандарта IEEE 802.1X-2004;
- на основе предварительно установленных ключей (*Pre-Shared key, PSK*).

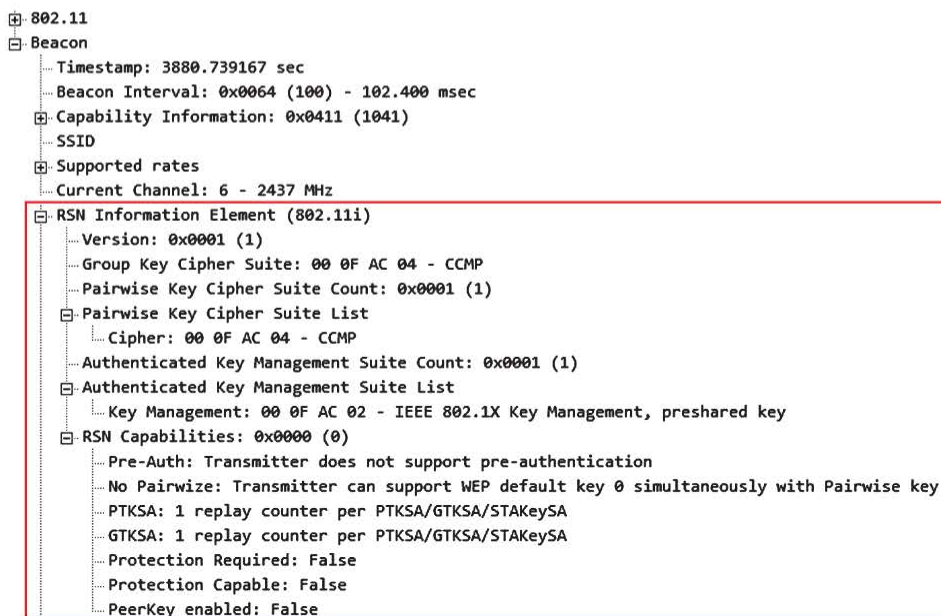


Рис. 3.6. Информация о возможностях безопасности в кадре Beacon

Стандарт 802.11 не навязывает никакой обязательной схемы аутентификации, поэтому производители оборудования могут использовать как небезопасные механизмы аутентификации, так и надежные. Выбор того или иного метода аутентификации зависит от требований к безопасности сети, типа пользователей, которые будут получать доступ к сети, типа данных, которые будут передаваться через нее. Но в любом случае обязательным условием для начала передачи кадров между станцией и точкой доступа является успешная ассоциация и аутентификация.

Аутентификация открытых систем и аутентификация с общим ключом относятся к методам аутентификации сетей, предшествующих сетям с усиленным режимом безопасности (*pre-RSN*), т. е. к методам, существовавшим в оригинальном стандарте IEEE 802.11 (аутентификация 802.11), имевшим множество уязвимостей и не обеспечивающим аутентификацию взаимодействующих устройств. В дополнение к методам безопасности, существовавшим в оригинальном стандарте, рабочая группа IEEE 802.11i разработала набор расширенных функций безопасности. В 2004 году стандарт IEEE 802.11i был

ратифицирован, и его финальная форма получила название *Robust Security Network (RSN)* — *сеть с усиленным режимом безопасности*. Для предоставления услуг аутентификации стандарт IEEE 802.11i опирается на IEEE 802.1X-2004 и механизм *четырёхстороннего рукопожатия (4-Way Handshake)*, позволяющий точкам доступа и беспроводным станциям безопасно обмениваться ключами шифрования.

Для обеспечения конфиденциальности и целостности данных в стандарте определены протоколы TKIP (*Temporal Key Integrity Protocol*) и CCMP (*CTR with CBC-MAC Protocol*). TKIP является необязательным и включен в стандарт для поддержки перехода с WEP на более надежные протоколы. CCMP обязателен для реализации. Он основан на алгоритме шифрования AES (*Advanced Encryption Standard*) и более устойчив к атакам. В 2007 году стандарт IEEE 802.11i был включен в стандарт IEEE 802.11–2007. Рассмотрим механизмы аутентификации 802.11 и RSN.

3.2.1. Аутентификация 802.11

В исходном стандарте IEEE 802.11 использовались два метода аутентификации: аутентификация открытых систем и аутентификация с общим ключом.

Аутентификация открытых систем (*Open System authentication*) или *открытая аутентификация* является так называемой нулевой аутентификацией, т. е. по сути не является механизмом аутентификации. В процессе аутентификации открытых систем происходит обмен двумя сообщениями (рис. 3.7):

1) станция, инициировавшая процесс аутентификации, отправляет точке доступа кадр аутентификации с номером последовательности 0x0001 (рис. 3.8), содержащий запрос аутентификации;

2) точка доступа отвечает станции кадром аутентификации с номером последовательности 0x0002 (рис. 3.9).

В случае успешной аутентификации код состояния в кадре устанавливается в значение «успех» (*successful*).

Никакой реальной проверки подлинности устройства, отправившего запрос на аутентификацию, с помощью этого механизма не производится. Стороны просто обмениваются информацией друг о друге: клиентское устройство отправляет запрос, точка доступа отвечает на него, после чего запускается процесс ассоциации (рис. 3.10).

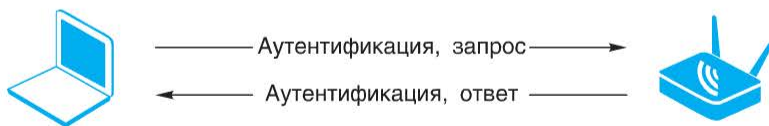


Рис. 3.7. Аутентификация открытых систем

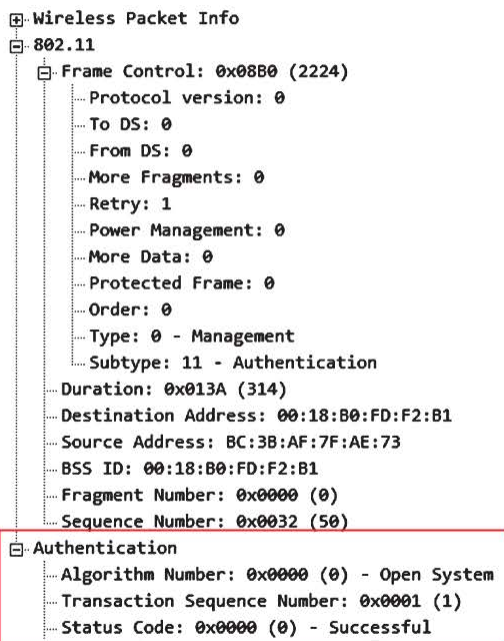


Рис. 3.8. Кадр запроса аутентификации со стороны клиента

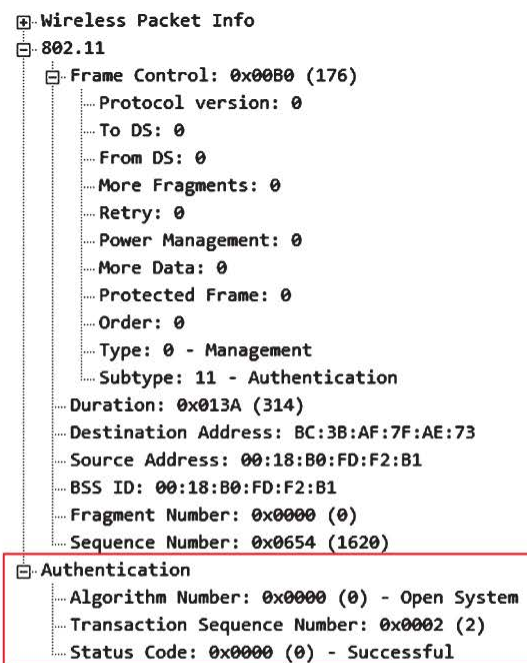


Рис. 3.9. Кадр ответа на запрос аутентификации

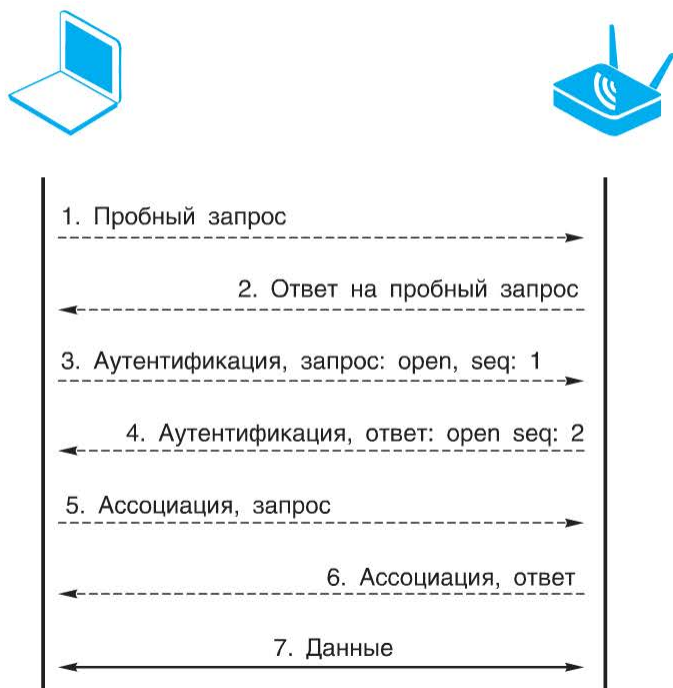


Рис. 3.10. Установление ассоциации после открытой аутентификации

Точка доступа может отказать в аутентификации клиентскому устройству только в том случае, если в его запросе указан метод, отличный от аутентификации открытых систем.

Таким образом, открытая аутентификация позволяет подключиться к беспроводной локальной сети любому клиентскому устройству. Открытую аутентификацию рекомендуется использовать в тех случаях, когда не требуется обеспечивать контроль доступа в сеть. Этот тип аутентификации используется при предоставлении доступа в Интернет через сети Wi-Fi в общественных местах (транспорте, парках и т. п.). Зачастую открытая аутентификация комбинируется с другими методами аутентификации и защиты информации.

В устаревших устройствах стандарта IEEE 802.11b аутентификация открытых систем может использоваться совместно с WEP для контроля доступа в сеть. Для этого секретные ключи WEP настраиваются заранее на точке доступа и клиентских устройствах. После успешной аутентификации и последующей ассоциации клиент может начать передачу данных. Однако если WEP-ключи клиента и точки доступа различаются, клиент не сможет ни передавать зашифрованные данные через точку доступа, ни дешифровывать данные, полученные от нее (рис. 3.11).

3. Подключение клиента к беспроводной сети...

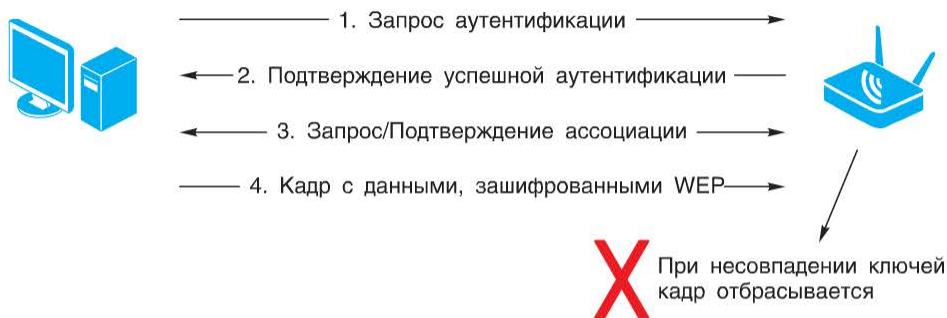


Рис. 3.11. Открытая аутентификация при использовании разных ключей WEP

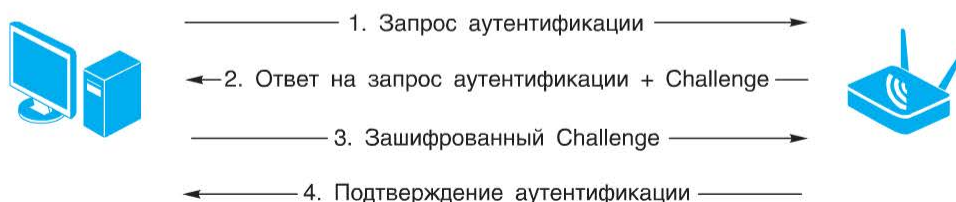


Рис. 3.12. Аутентификация с общим ключом

В современных устройствах такая функциональность поддерживается только для совместимости с устаревшим оборудованием стандарта IEEE 802.11b.

В отличие от открытой аутентификации *аутентификация с общим ключом* (*Shared Key authentication*) может использоваться только совместно с протоколом WEP. Она требует, чтобы две стороны совместно владели общим секретным ключом, не доступным третьей стороне. Другими словами, при аутентификации с общим ключом требуется, чтобы точка доступа и клиентское устройство поддерживали WEP и имели одинаковые ключи WEP. Процесс аутентификации выполняется путем обмена четырьмя кадрами (рис. 3.12):

1) клиент посылает точке доступа запрос аутентификации, указывая при этом необходимость использования режима аутентификации с общим ключом;

2) точка доступа отвечает кадром аутентификации, который содержит так называемый Challenge, представляющий собой строку символов, созданную с помощью генератора случайных чисел;

3) клиент отправляет обратно точке доступа кадр аутентификации, шифрованный ключом WEP и включающий полученный от нее Challenge;

4) точка доступа получает шифрованный кадр и дешифрует его, используя свой ключ WEP. При успешной дешифровке полученного кадра сравнивается принятый Challenge с текстом, отправленным на втором этапе процедуры. Если текст совпал, точка доступа посылает клиенту сообщение аутентификации, содержащее код состояния «успех» (*successful*). В противном случае сообщение будет содержать код состояния «неудача» (*unsuccessful*).

В настоящее время не рекомендуется использовать данный метод аутентификации в связи с обнаруженными в нем уязвимостями.

После успешной аутентификации открытых систем или аутентификации с общим ключом устройство переходит в состояние «аутентифицировано, не ассоциировано». Следующим шагом становится ассоциация с точкой доступа.

3.2.2. Ассоциация после аутентификации 802.11

После успешной аутентификации 802.11 (открытой или с общим ключом) станция начинает процесс ассоциации с точкой доступа (рис. 3.13). Для этого она отправляет точке доступа *запрос ассоциации* (*Association Request*)

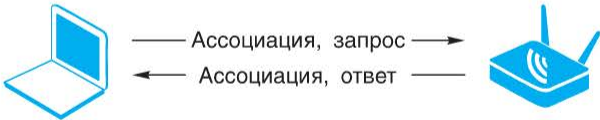


Рис. 3.13. Ассоциация

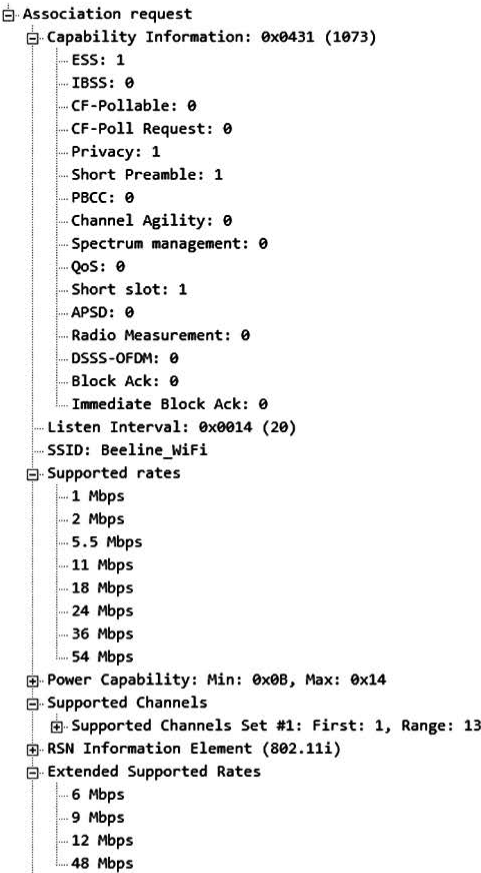


Рис. 3.14. Запрос на ассоциацию
Association Request

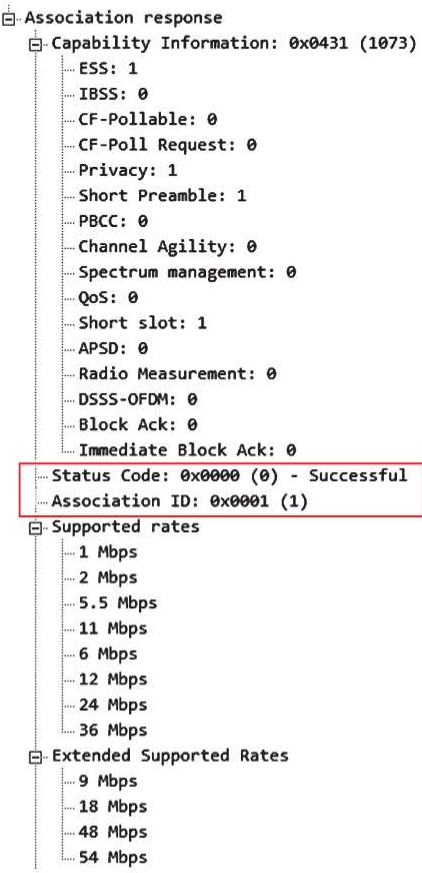


Рис. 3.15. Ответ на запрос ассоциации
Association Response

(рис. 3.14), содержащий информацию о своих возможностях. Точка доступа получает запрос и проверяет, совпадают ли ее возможности с возможностями станции. При совпадении создает для станции *идентификатор ассоциации* (*Association Identifier, AID*), затем отправляет ей ответ на запрос ассоциации (*Association Response*) (рис. 3.15), содержащий код состояния «успех» (*successful*) и значение AID. В случае неудачи код состояния ответа на запрос ассоциации будет содержать код причины отказа.

После успешного завершения этапа ассоциации станция переходит в четвертое состояние «аутентифицировано и ассоциировано» и становится полноправным членом беспроводной сети.

3.3. Аутентификация RSN и безопасная ассоциация

Аутентификация RSN и обмен ключами шифрования позволяют осуществлять *безопасную ассоциацию* (*Robust Security Network Association, RSN*). Аутентификация RSN включает следующие методы:

- аутентификацию на основе предварительно установленных ключей (PSK);
- аутентификацию на основе стандарта IEEE 802.1X.

Аутентификация на основе стандарта IEEE 802.1X обеспечивает взаимную аутентификацию точки доступа и беспроводной станции. При аутентификации на основе PSK под взаимной аутентификацией подразумевается владение точкой доступа и станцией общим секретом.

Напомним, что станция узнает о функциях безопасности, поддерживаемых точкой доступа, из кадров *Beacon* или *Probe Response* в процессе пассивного или активного сканирования. Функции безопасности указываются в элементе RSN IE (*Robust Security Network Information Element*), содержащемся в этих кадрах (см. рис. 3.6).

3.3.1. Аутентификация на основе стандарта IEEE 802.1X

Аутентификация на основе стандарта IEEE 802.1X требует предварительного успешного выполнения открытой аутентификации и ассоциации. Открытая аутентификация выполняется с целью обеспечения обратной совместимости с машиной состояний 802.11. Цель последующей ассоциации — согласование набора возможностей обеспечения безопасности, которые будут использоваться. Возможности обеспечения безопасности — это поддерживаемые протоколы конфиденциальности и целостности данных, методы аутентификации и схемы управления ключами шифрования. Станция отправляет точке доступа запрос на ассоциацию, который содержит перечень установленных на ней параметров безопасности. Если параметры безопасности точки доступа и станции не совпали, точка доступа отвечает отказом в ассоциации. Получив положительный ответ на запрос ассоциации, станция перейдет в третье состояние «аутентифицировано и ассоциировано» и начнет выполнение аутентификации 802.1X (рис. 3.16).

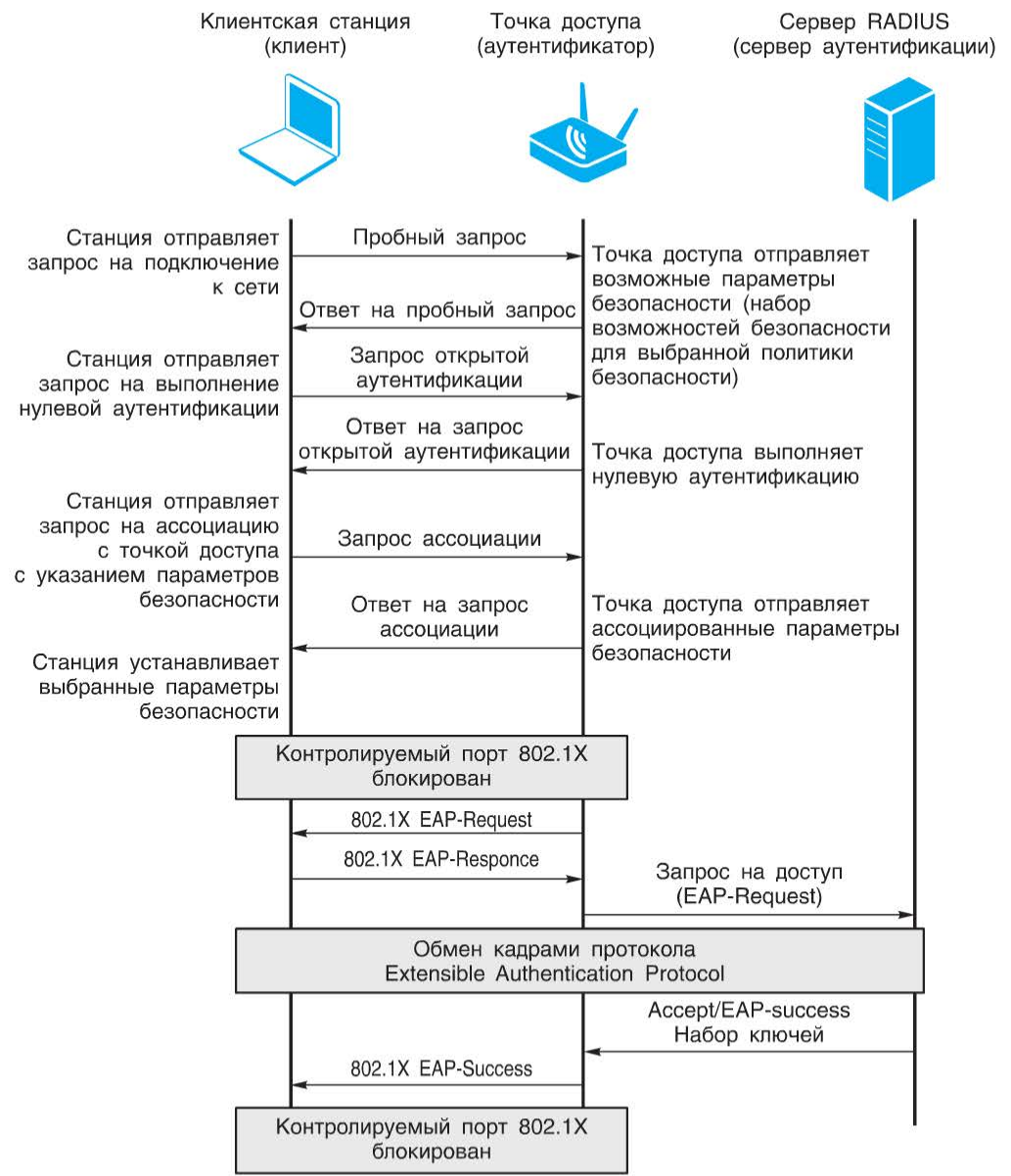


Рис. 3.16. Фазы безопасной ассоциации RSN: сканирование, открытая аутентификация, ассоциация, аутентификация 802.1X

Стандарт IEEE 802.1X разработан институтом IEEE для управления доступом на основе портов в сетях IEEE 802 (LAN и WLAN). Он описывает использование протокола EAP (*Extensible Authentication Protocol*) для поддержки аутентификации с помощью сервера аутентификации и определяет процесс

инкапсуляции данных EAP, передаваемых между клиентами (запрашивающими устройствами) и серверами аутентификации. Стандарт IEEE 802.1X обеспечивает контроль доступа и не позволяет неавторизованным устройствам подключаться к локальной проводной или беспроводной сети через порты устройства связи (в проводных сетях — через порты коммутаторов или маршрутизаторов; в беспроводных сетях интерфейсом для приема и передачи волн является антенна).

Точка доступа, используя процесс ассоциации, присваивает беспроводной станции идентификатор ассоциации (AID), который можно рассматривать как логический порт. При реализации защиты от подключения к сети неавторизованных клиентских устройств путем аутентификации на основе портов порт устройства связи сначала помещается в состояние «заблокирован» и через него возможна передача только идентификационной информации клиента, например логина и пароля. Идентификационная информация не может пересылаться по сети в открытом виде, поэтому для ее передачи используется специальный протокол Extensible Authentication Protocol (EAP). Если аутентификация проходит успешно, запускается генерация и обмен ключами шифрования, порт разблокируется и клиентскому устройству предоставляется доступ в сеть. После этого он может начать передачу обычного трафика.

В стандарте IEEE 802.1X определены три роли устройств в общей схеме аутентификации:

- клиент (*Client/Supplicant*);
- аутентификатор (*Authenticator*);
- сервер аутентификации (*Authentication Server*).

Опишем эти роли в беспроводных сетях.

Клиент (*Client/Supplicant*) — это станция, запрашивающая доступ к беспроводной локальной сети и отвечающая на запросы точки доступа. Для этого на станции используется клиентское ПО протокола 802.1X, встроенное в ОС клиентского компьютера или установленное дополнительно.

Сервер аутентификации (*Authentication Server*) выполняет фактическую аутентификацию клиента: проверяет подлинность клиента и информирует точку доступа о предоставлении или отказе клиенту в доступе к сети. В качестве сервера аутентификации обычно используется сервер RADIUS (*Remote Authentication Dial-In User Service*).

Аутентификатор (*Authenticator*) управляет физическим доступом к сети, основываясь на статусе аутентификации клиента. Эту роль выполняет точка доступа. Она работает как посредник (*Proxy*) между клиентом и сервером аутентификации: получает запрос на проверку подлинности от клиента, проверяет данную информацию при помощи сервера аутентификации и пересылает ответ клиенту. Точка доступа реализует функциональность клиента RADIUS, который отвечает за инкапсуляцию и деинкапсуляцию кадров EAP и взаимодействие с сервером аутентификации.

Remote Authentication Dial-In User Service (RADIUS) — сетевой протокол, обеспечивающий централизованное управление аутентификацией, авторизацией и ведением журналов доступа учетных записей пользователей (*Authentication, Authorization, Accounting (AAA)*), подключающихся к сети и использующих ее сервисы. Описан в RFC 2865 и RFC 2866.

Инициировать процесс аутентификации может как точка доступа, так и клиентская станция. Процесс начинается когда аутентификатор посылает клиенту кадр запроса на идентификацию EAP-Request или клиент отправляет точке доступа кадр EAPOL-start, вынуждая ее отправить ему запрос EAP-Request. При ответе клиента кадром EAP-Response со своей идентификационной информацией точка доступа начинает играть роль посредника, передающего кадры EAP между клиентом и сервером аутентификации до успешной или неудачной аутентификации. Схема обмена EAP-кадрами зависит от используемого метода аутентификации. В рамках протокола EAP могут быть реализованы различные методы проверки подлинности пользователя, например, такие как EAP-TLS (*EAP-Transport Layer Security*) или EAP-PEAP (*EAP-Protected EAP*).

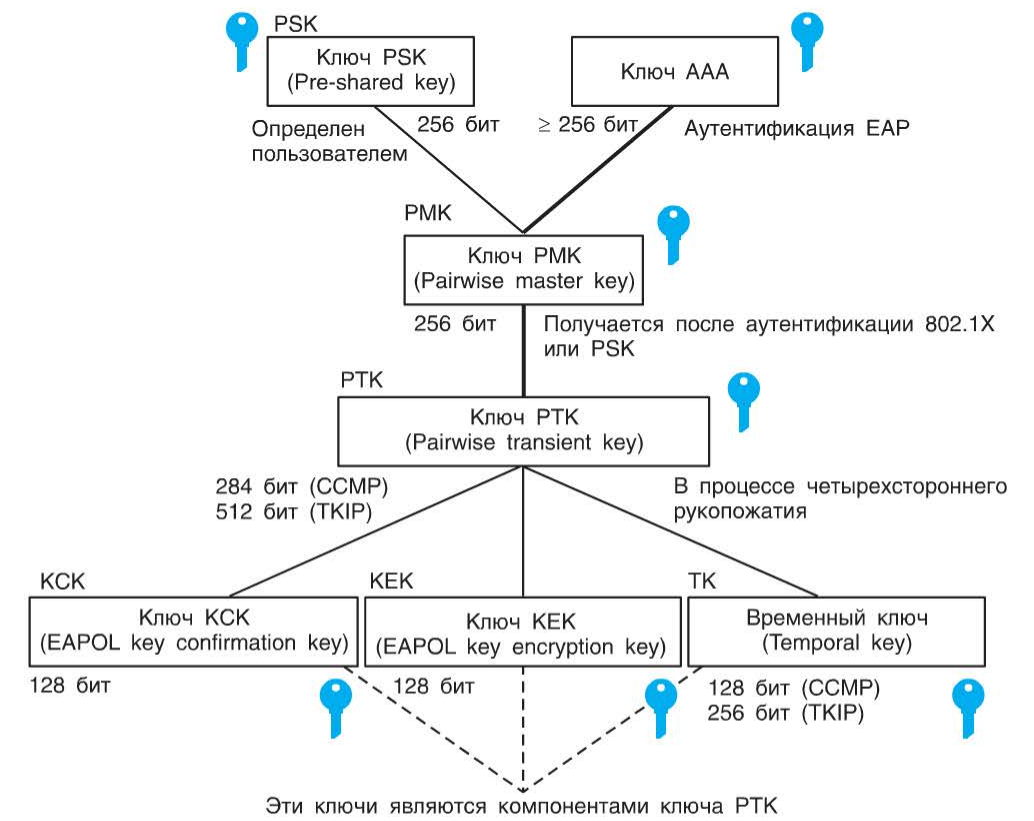


Рис. 3.17. Иерархия ключей

В последней фазе аутентификации сервер аутентификации и клиент генерируют *парный мастер-ключ (Pairwise Master Key, PMK)* на основе заранее сконфигурированного симметричного *мастер-ключа (Master Key, МК)*. После того как сервер аутентификации отправил PMK аутентификатору, аутентификация успешно завершается, но логический порт точки доступа все еще остается заблокированным для станции.

PMK не используется для шифрования или дешифрования данных. Он служит для генерации группы ключей во время *процесса четырехстороннего рукопожатия (4-Way Handshake)*, который начинается сразу после успешной аутентификации. Процесс четырехстороннего рукопожатия позволяет провести безопасный обмен парными ключами шифрования между точкой доступа и станцией.

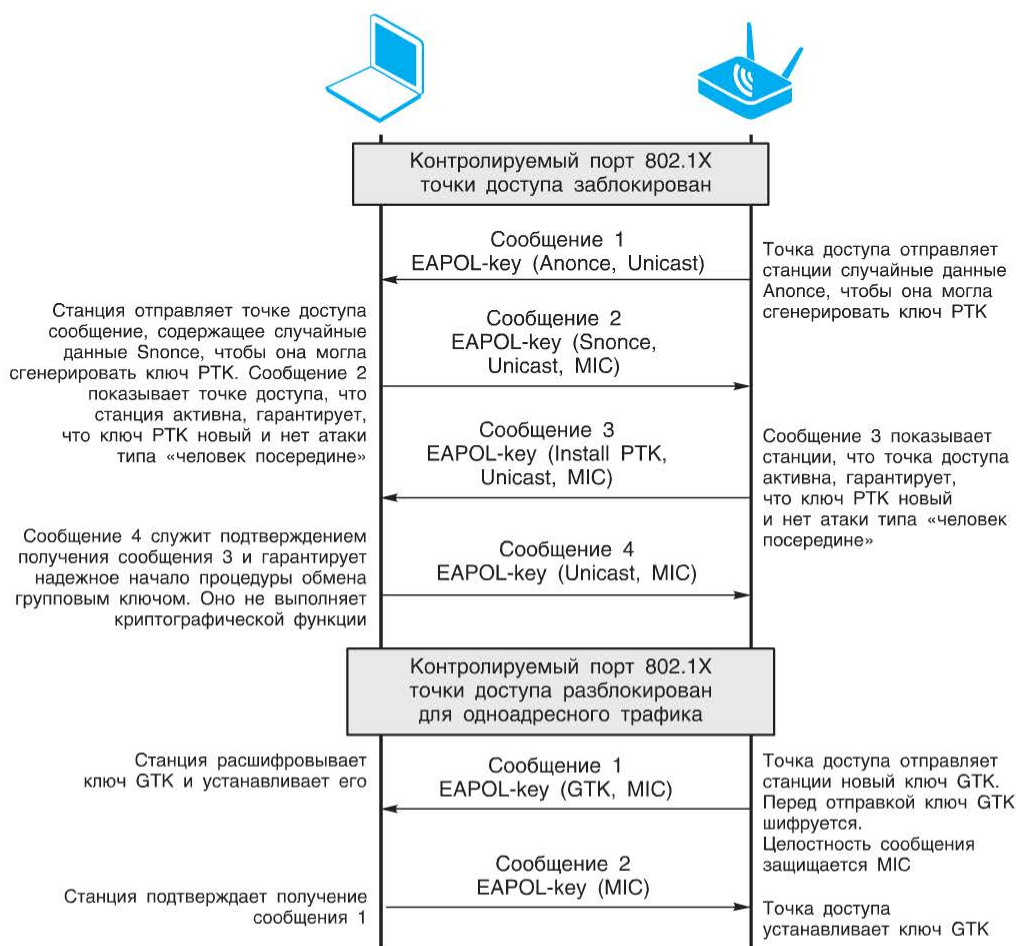


Рис. 3.18. Процесс четырехстороннего рукопожатия

PMK, сгенерированный на последней фазе аутентификации, используется для генерации *парного временного ключа (Pairwise Transient Key, PTK)*, который является составным и включает в себя три ключа (рис. 3.17):

- *EAP Over LAN Key Confirmation Key (EAPOL-KCK)* — ключ подтверждения ключа (биты PTK с номерами от 0 до 127), используемый для защиты целостности ключей, распределяемых между станцией и точкой доступа в процессе четырехстороннего рукопожатия;
- *EAP Over LAN Key Encryption Key (EAPOL-KEK)* — ключ шифрования ключа (биты PTK с номерами от 128 до 255), используемый для шифрования *группового временного ключа (Group Temporal Key, GTK)* и других ключей, распределяемых между станцией и точкой доступа в процессе четырехстороннего рукопожатия;
- *Temporal Key (TK)* — временный ключ (биты PTK с номерами от 256 и выше), используемый с TKIP или CCMP для шифрования одноадресного пользовательского трафика.

Генерация PTK проходит в четыре этапа (рис. 3.18).

1. Аутентификатор посылает клиенту сообщение EAPOL-key (рис. 3.19), содержащее MAC-адрес точки доступа и случайные данные, называемые *Anonce*.
2. Клиент генерирует свои собственные случайные данные *Snonce*. Для генерации PTK клиент использует случайные данные *Anonce* и *Snonce*, индивидуальные MAC-адреса (свой и точки доступа), а также PMK. Далее клиент отправляет сообщение EAPOL-key, содержащее его индивидуальный MAC-адрес и случайные данные *Snonce*, позволяя точке доступа сгенерировать точно такой же ключ PTK. Это сообщение включает *код целостности сообщения (Message Integrity Code, MIC)* с ключом KCK.

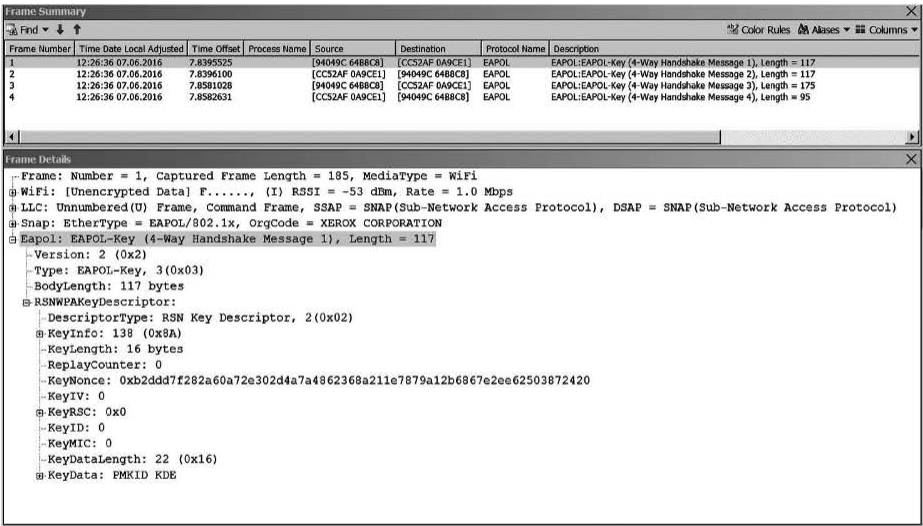


Рис. 3.19. Кадры EAPOL-key

3. Аутентификатор генерирует ключ РТК. Если не возникло ошибок, точка доступа отправляет клиенту сообщение EAPOL-key о применении РТК и включает в него код целостности сообщения (MIC).

4. Клиент отправляет аутентификатору сообщение EAPOL-key, подтверждающее использование данного ключа. Для защиты сообщения используется MIC.

Для того чтобы станция, ассоциированная с точкой доступа, могла дешифровать отправленный ей групповой или широковещательный трафик, используется *групповой временный ключ (Group Temporal Key, GTK)*, который генерируется точкой доступа и передается ассоциированной с ней станции. В отличие от РТК распространение GTK происходит в два этапа, так как его доставка выполняется через безопасное соединение, после того как переданы все парные ключи. Аутентификация в данном случае не требуется:

1) в первом сообщении точка доступа отправляет станции ключ GTK, зашифрованный с помощью алгоритмов RC4 или AES. Для шифрования используется ключ КЕК. Целостность сообщения защищается с помощью MIC;

2) станция подтверждает получение GTK. Это сообщение также содержит MIC.

Точка доступа может выполнять генерацию нового ключа GTK по ряду причин, например при отключении станции.

При успешном завершении процесса четырехстороннего рукопожатия аутентификатор и клиент считают, что успешно аутентифицировали друг друга, порт точки доступа разблокируется и станция может начинать передачу данных.

В связи со сложностью аутентификации 802.1X она используется в основном в больших корпоративных сетях, где требуется контролировать доступ в сеть множества пользователей. В домашних сетях или сетях небольших офисов используется более простой вариант аутентификации на основе предварительно установленных ключей (PSK).

3.3.2. Аутентификация на основе предварительно установленных ключей (PSK)

Аутентификация на основе предварительно установленных ключей является самым распространенным способом аутентификации, используемым в домашних сетях и сетях небольших офисов. При аутентификации на основе PSK на точке доступа и группе подключаемых к ней клиентских станций требуется настройка общего секрета, вид которого определяется используемым ПО системы. Секрет можно ввести в виде строки из 64 шестнадцатеричных символов или в виде парольной фразы, содержащей от 8 до 63 ASCII-символов. Для того чтобы создать ключ PSK длиной 256 бит используется специальная функция формирования ключей, входными данными для которой являются секрет, SSID сети, в которой используется этот секрет, длина SSID, количество итераций хэширования и длина ключа. Формирование ключа PSK выполняется до процесса обмена кадрами аутентификации.

Начать процесс аутентификации может как точка доступа, так и станция, при этом они могут это сделать одновременно (рис. 3.20).

После того как станция получает информацию о политиках безопасности точки доступа из кадра *Beacon* или с помощью активного сканирования, стороны обмениваются двумя кадрами аутентификации 802.11 с номерами последовательностей 0x0001 и 0x0002 и отправляют друг другу сообщение *Commit*, в котором содержится предполагаемый секретный ключ другой стороны. В ответ на это сообщение, если секретный ключ совпал, каждая из сторон посылает сообщение *Confirm* с подтверждением.

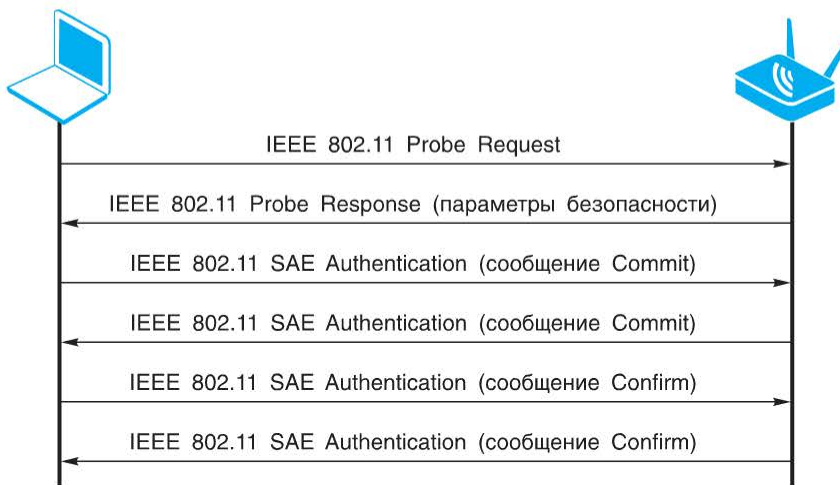


Рис. 3.20. Процесс аутентификации на основе PSK

После успешной аутентификации точка доступа и станция генерируют из ключа PSK ключ PMK. Затем станция ассоциируется с точкой доступа и осуществляется договоренность о политиках безопасности.

Сгенерированный в процессе аутентификации ключ PMK используется в процессе четырехстороннего рукопожатия для генерации ключа PTK (см. рис. 3.18). Для шифрования и дешифрования широковещательного и группового трафика точкой доступа генерируется ключ GTK и доставляется на ассоциированную с ней станцию. После завершения этого процесса станция становится членом беспроводной сети и может начать безопасную передачу данных.

3.4. Дополнительные методы контроля доступа к беспроводной сети

В беспроводных сетях могут использоваться механизмы контроля доступа, выходящие за рамки стандарта IEEE 802.11. Контроль над подключением клиента к точке доступа на основе его MAC-адреса стандартом IEEE 802.11 не предусмотрен, однако поддерживается многими производителями оборуду-

3. Подключение клиента к беспроводной сети...

дования для беспроводных сетей. Для этого точка доступа должна поддерживать функцию *фильтрации по MAC-адресам* (*MAC Filtering*), которая позволяет разрешать или запрещать подключение клиентов к сети на основе их MAC-адресов. Администратор может настроить на точке доступа список разрешенных или запрещенных MAC-адресов. При попытке подключения беспроводного клиента точка доступа проверяет заранее сконфигурированный список и определяет, разрешено ли этому клиенту подключаться к сети или нет (рис. 3.21).

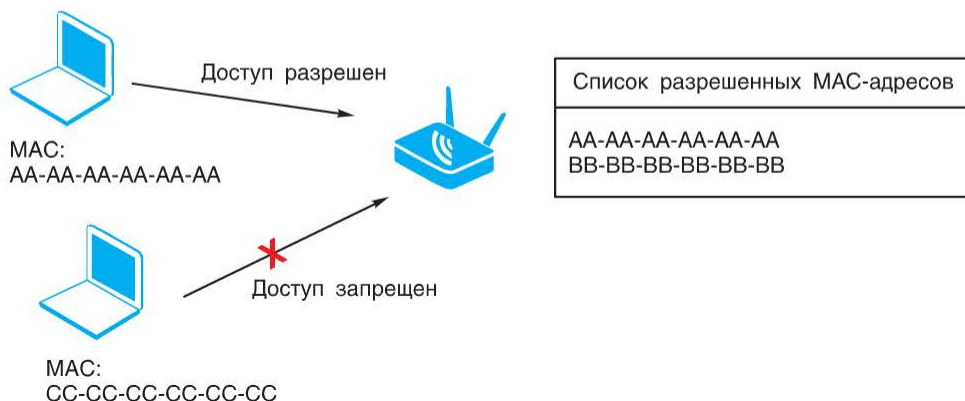


Рис. 3.21. Фильтрация клиентов по MAC-адресам

Функция фильтрации по MAC-адресам может использоваться совместно с механизмами аутентификации, например открытой аутентификацией или аутентификацией с общим ключом.

При использовании этого метода существуют уязвимости, связанные с тем, что в кадре MAC-адреса клиента и точки доступа передаются в открытом виде. В результате этого злоумышленник может определить разрешенные MAC-адреса и подменить MAC-адрес своего устройства на легитимный. Подмена MAC-адреса возможна в беспроводных адаптерах, допускающих использование локально администрируемых MAC-адресов. Для выявления MAC-адресов легитимных клиентов злоумышленник может воспользоваться анализатором трафика протокола IEEE 802.11.

4. Безопасность передачи данных в беспроводных сетях

В проводных сетях передавать и получать данные могут только физически подключенные к сети станции. В беспроводных сетях передавать и получать данные может любая станция, находящаяся в пределах досягаемости радиосвязи других устройств. Таким образом, проводные сети в некоторой степени обеспечивают конфиденциальность данных, ограничивая число возможных получателей данных устройствами, физически подключенными к сети. Для того чтобы приблизить уровень безопасности беспроводных сетей к уровню безопасности проводных сетей, в стандарте IEEE 802.11 определены возможности защиты содержимого передаваемых сообщений. Предотвращение чтения сообщений теми, кому они не предназначаются, обеспечивается услугой конфиденциальности данных.

Для обеспечения конфиденциальности и целостности данных в стандарте IEEE 802.11 предусмотрены протоколы шифрования WEP, TKIP и CCMP. Протокол WEP относится к средствам безопасности беспроводных сетей, существовавшим в оригинальном стандарте IEEE 802.11. В настоящее время не рекомендуется использование протокола WEP в связи с его криптографической уязвимостью, но его поддержка присутствует в современном оборудовании для обратной совместимости с устаревшими устройствами. Протоколы TKIP и CCMP относятся к средствам безопасности RSN и определены в стандарте IEEE 802.11i-2004.

4.1. Протокол WEP

WEP (*Wired Equivalent Privacy*) — алгоритм обеспечения конфиденциальности и целостности данных, определенный в оригинальном стандарте IEEE 802.11. Конфиденциальность и целостность данных обеспечиваются на основе алгоритма симметричного потокового шифрования RC4 (Rivest's Cipher v.4, код Ривеста).

Алгоритм WEP работает по принципу электронной кодовой книги, в которой каждый блок открытого текста заменяется блоком шифрованного текста. Шифрование начинается после передачи секретных ключей взаимодействующим устройствам. Поскольку WEP является симметричным алгоритмом шифрования, один и тот же ключ используется как для шифрования, так и для дешифрования передаваемых данных (рис. 4.1).

WEP использует ключи длиной 40 и 104 бит. Они задаются вручную при настройке шифрования на точках доступа и клиентских устройствах. Ключ длиной 40 бит представляет собой 5 ASCII-символов или 10 шестнадцатеричных чисел. Ключ длиной 104 бит представляет собой 13 ASCII-символов или 26 шестнадцатеричных чисел. При этом обмен пользовательскими данными между взаимодействующими устройствами возможен только в том случае, если они используют одинаковые ключи шифрования. В противном

случае клиент не сможет правильно шифровать передаваемые данные и они будут отброшены точкой доступа или дешифровать кадры, полученные от точки доступа.

К секретному ключу длиной 40 или 104 бит присоединяется *вектор инициализации (Initialization Vector, IV)* длиной 24 бита, выбираемый случайным образом и динамически изменяющийся при каждой передаче. Таким образом получаются ключи длиной 64 и 128 бит ($40 + 24 = 64$, $104 + 24 = 128$), указываемые производителями оборудования в характеристиках устройств.



Рис. 4.1. Схема симметричного шифрования

Секретный ключ вместе с вектором инициализации подается на вход генератора псевдослучайных чисел (PRNG), выдающего ключевую последовательность, длина которой равна длине кадра MAC с присоединенной к нему 32-битовой последовательностью циклической проверки четности с избыточностью (CRC-32). Последовательность CRC вычисляется с помощью алгоритма обеспечения целостности. Побитовое применение операции исключающего ИЛИ (XOR) к псевдослучайной ключевой последовательности и кадру MAC с CRC дает зашифрованный текст. К данному тексту присоединяется вектор инициализации в открытом виде (чтобы принимающая сторона могла успешно дешифровать кадр) и сообщение передается по сети (рис. 4.2). Так как вектор инициализации меняется при каждой передаче, то изменяется и генерируемая ключевая последовательность. Таким образом, один и тот же кадр, передаваемый многократно, каждый раз будет порождать уникальный зашифрованный кадр.

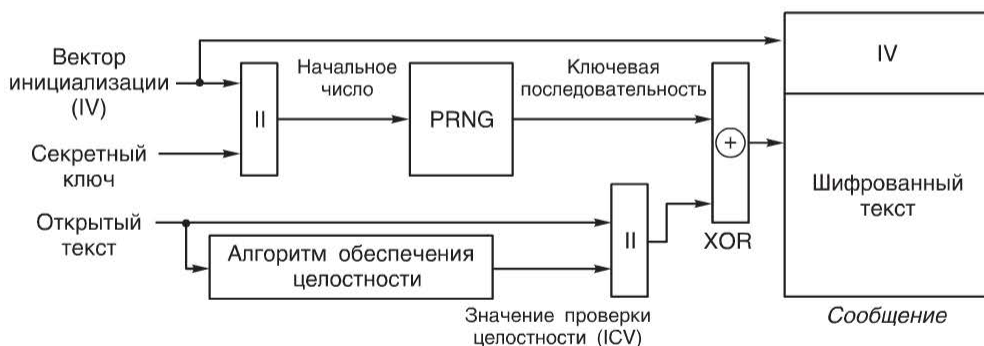


Рис. 4.2. Процесс шифрования WEP

Дешифрование состоит в восстановлении ключевой последовательности, с помощью которой был зашифрован переданный текст. После получения сообщения получатель извлекает из него вектор инициализации и присоединяет его к совместно используемому секретному ключу, после чего генерирует ту же псевдослучайную последовательность, что и отправитель. Далее к восстановленной ключевой последовательности и полученному зашифрованному кадру побитово применяется операция исключающего ИЛИ, результатом которой является исходный текст.

Криптоаналитиками было установлено, что ключ WEP может быть вычислен с использованием определенных кадров, собранных пассивным прослушиванием беспроводной локальной сети. Причиной уязвимости послужила реализация в WEP *метода планирования ключей (Key Scheduling Algorithm, KSA)* алгоритма потокового шифрования RC4. Некоторые векторы инициализации (так называемые слабые векторы) дают возможность установить побитовый состав ключа, применяя статистический анализ собранных данных.

Подобная уязвимость делает шифрование с использованием WEP неэффективным, лишая его криптографической стойкости. Однако если оборудование не поддерживает современные механизмы обеспечения конфиденциальности и целостности данных, то для повышения защищенности сети желательно использовать WEP с максимальной длиной ключа (128 бит или выше), а также задействовать возможность циклической смены WEP-ключей из списка (возможность настроить список из четырех ключей WEP, которые будут циклически меняться), если оборудование поддерживает эту функцию, или вручную менять ключи не реже одного раза в месяц.

4.2. Протокол TKIP

Протокол TKIP (*Temporal Key Integrity Protocol* — протокол целостности временного ключа) был разработан с целью изменения программного обеспечения устройств, аппаратная часть которых способна поддерживать только протокол WEP. TKIP усиливает криптографическую стойкость WEP благодаря использованию нескольких дополнительных функций. Протокол TKIP предоставляет два сервиса:

- целостность сообщений: отправитель вычисляет *код целостности сообщения (Message Integrity Code, MIC)*, защищенный ключом, и добавляет его в кадр 802.11 после поля данных. MIC создается с помощью протокола Michael, вычисляющего 64-битовое значение, используя в качестве входных параметров MAC-адреса отправителя (SA) и получателя (DA), приоритет, передаваемые данные, а также ключ MIC. Получатель проверяет MIC после дешифрования и отбрасывает сообщения с неверным значением MIC. Вычисление MIC позволяет противодействовать атакам типа *forgery* (изменение содержимого передаваемых пакетов);

- конфиденциальность данных: для шифрования данных и MIC используется алгоритм RC4. При динамической генерации ключа RC4 для каждого передаваемого кадра TKIP используется криптографическая функция перемешивания, состоящая из двух фаз (рис. 4.3).



Рис. 4.3. Процесс шифрования TKIP

Для дополнительной защиты каждого передаваемого кадра TKIP использует *счетчик последовательности (TKIP sequence counter, TSC)* длиной 48 бит. TSC служит двум целям. Во-первых, он позволяет противодействовать атакам типа *replay*, основанным на повторном использовании ключей, так как получатель будет отбрасывать кадры, пришедшие не по порядку. Во-вторых, TSC объединяется с временным ключом с целью генерации динамического ключа шифрования для каждого передаваемого кадра, т. е. выступает в роли вектора инициализации WEP (WEP IV) и расширенного вектора инициализации (Extended IV).

В отличие от WEP, использующего статический базовый ключ, в TKIP применяется усовершенствованный механизм управления ключами. TKIP использует временные ключи, которые генерируются в процессе аутентификации на основе стандарта IEEE 802.1X или на основе PSK. Напомним, что сгенерированный в процессе аутентификации ключ РМК используется механизмом четырехстороннего рукопожатия для генерации ключа РТК, который является составным и включает несколько ключей. *Временный ключ (Temporal Key, TK)* длиной 256 бит используется с TKIP следующим образом: два 64-битовых ключа — с алгоритмом Michael для генерации MIC, один ключ — для защиты сообщений, передаваемых точкой доступа станции, другой ключ — для защиты сообщений, передаваемых станцией точке доступа, остальные 128 бит применяются для генерации покадрового ключа RC4, используемого для шифрования передаваемых данных.

Процесс формирования ключа шифрования для каждого кадра состоит из двух фаз. В первой фазе смешиваются соответствующий временный ключ длиной 128 бит (TK), MAC-адрес отправителя (*Transmitter Address, TA*) и старшие 32 бит счетчика последовательности (TSC). В результате смешения получается ключ первой фазы длиной 80 бит, который с целью повышения производительности станция может занести в кэш. Этот ключ можно исполь-

зовать повторно для передачи кадров, ассоциированных с данным ТК и MAC-адресом отправителя. Во второй фазе ключ первой фазы смешивается с младшими 16 бит счетчика последовательности (TSC) и временным ключом. В результате смещения получается покадровый ключ длиной 128 бит, который можно использовать для шифрования данных.

Поскольку TKIP основан на WEP, требуется, чтобы вектор инициализации присутствовал в открытом виде в заголовке зашифрованного кадра (рис. 4.4). Вектор инициализации состоит из 24 бит. Первый и третий октет вектора инициализации содержат младшие 16 бит счетчика последовательности, оставшиеся 32 бит счетчика TSC находятся в поле расширенного вектора инициализации (*Extended IV*), следующего за полем IV.

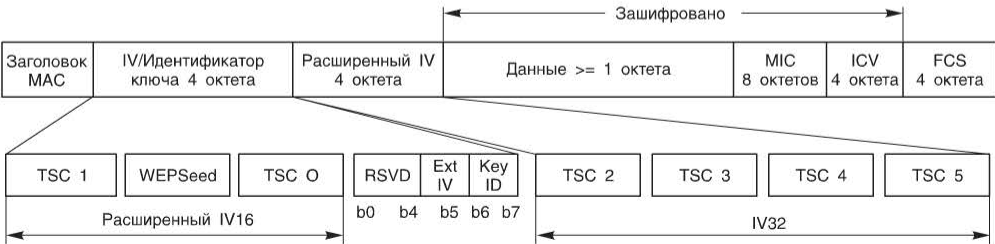


Рис. 4.4. Формат кадра TKIP

В целом механизм шифрования TKIP функционирует следующим образом:

- 1) для каждого передаваемого кадра вычисляется значение MIC, которое добавляется к полю данных;

- 2) если необходимо, кадр с уже вычисленным значением MIC разбивается на фрагменты;

- 3) каждому кадру назначается монотонно увеличивающееся значение TSC, при этом фрагменты одного кадра имеют одинаковое значение расширенного вектора инициализации (32 старших бит счетчика последовательности);

- 4) для каждого кадра с помощью двухфазной криптографической функции перемешивания генерируется покадровый ключ;

- 5) каждый кадр или фрагмент кадра шифруется с помощью покадрового ключа и передается по сети.

Процесс дешифрования кадра состоит из следующих шагов (рис. 4.5):

- 1) из полей IV и *Extended IV* полученного кадра получатель извлекает значение счетчика последовательности. Если оно не соответствует правилам последовательности, то кадр или фрагмент кадра отбрасывается;

- 2) вычисляется ключ первой фазы, затем вычисляется ключ второй фазы, с помощью которого расшифровывается кадр или фрагмент кадра;

- 3) осуществляется проверка контрольной суммы кадра (ICV). В случае отрицательного результата проверки кадр отбрасывается;

- 4) если кадр был фрагментирован, то расшифрованные фрагменты кадра собираются в исходный кадр. Если этого не происходит, кадр отбрасывается;

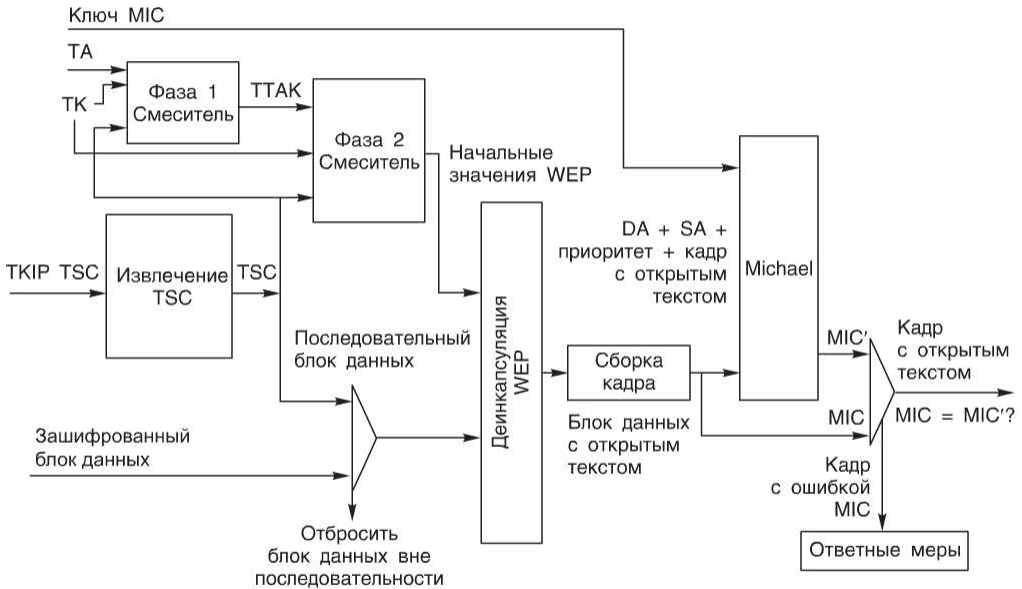


Рис. 4.5. Процесс дешифрования кадра TKIP

5) получатель на основании MAC-адресов отправителя и получателя, приоритета, данных вычисляет значение MIC' и сравнивает его со значением, находящимся в поле MIC кадра;

6) если эти значения совпадают, кадр обрабатывается получателем;

7) если эти значения не совпадают, получатель отбрасывает кадр и принимает соответствующие меры по обработке сложившейся ситуации.

Несмотря на то что TKIP усиливает стойкость WEP за счет использования двухфазной криптографической функции перемешивания, вычисления MIC и применения TSC, в его основе лежит тот же самый слабый криптографический алгоритм RC4, что делает TKIP уязвимым для большинства атак аналогично WEP.

4.3. Протокол CCMP

Протокол CCMP (*CTR with CBC–MAC Protocol*) является обязательным для реализации протоколом работы современных беспроводных устройств и основан на режиме CCM (*Counter Mode with CBC–MAC*) алгоритма шифрования AES (*Advanced Encryption Standard*).

Инициатива в разработке AES принадлежит Национальному институту стандартов и технологий (NIST) США, который предложил сообществу криптологов разработать новые алгоритмы шифрования с целью создания полностью открытого и бесплатного алгоритма симметричного шифрования, доступного для широкого применения. Требования к алгоритму: симметричный, блочный, должен поддерживать длину блока 128 бит и длину ключа 128,

192 и 256 бит. В результате длительного процесса оценки предложенных алгоритмов в качестве AES был выбран алгоритм Rijndael и определен в FIPS PUB 197–2001.

При рассмотрении возможностей усиления механизмов шифрования данных в беспроводных сетях институт IEEE адаптировал алгоритм AES специально для них.

Режим CCM (определен в IETF RFC 3610) представляет собой комбинацию режима *счета* блоков шифра (*CTR, counter*) и *кода аутентификации сообщения из блочного шифра* (*Cipher Block Chaining Message Authentication Code, CBC-MAC*). Эти режимы используются для предоставления двух сервисов:

- целостность сообщений: для обеспечения целостности и аутентификации CCMP использует CBC-MAC. При этом защищается целостность не только данных, но и выбранной части заголовка кадра;
- конфиденциальность данных: для шифрования CCMP использует режим CTR.

Для обеспечения конфиденциальности и целостности используется один и тот же ключ AES длиной 128 бит. CCM требует «свежий» временный ключ для каждой сессии и уникальные случайные данные (*nonce*) для каждого кадра, защищаемого данным временным ключом. Для создания *nonce* используется номер пакета (PN) длиной 48 бит, что позволяет избежать атак типа *replay*. Напомним, что временный ключ генерируется в процессе аутентификации на основе стандарта IEEE 802.1X или PSK.

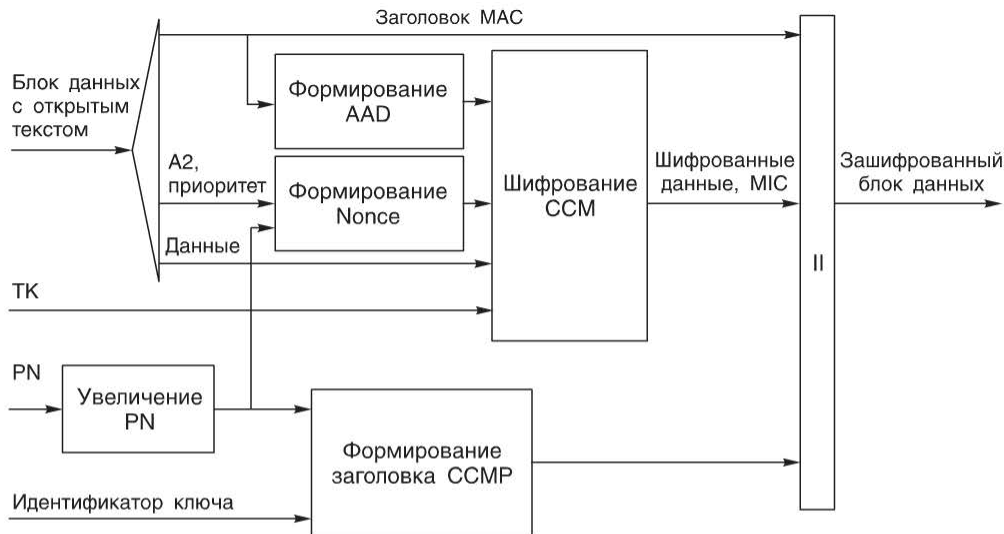


Рис. 4.6. Процесс шифрования CCMP

Механизм шифрования CCMP функционирует следующим образом (рис. 4.6):

- 1) для каждого кадра увеличивается значение номера пакета (PN) (получение «свежего» PN), что позволяет не использовать значение PN для одного и того же временного ключа повторно;

2) из полей заголовка оригинального кадра для алгоритма CCM формируются *дополнительные данные аутентификации (Additional Authentication Data, AAD)*. В формировании AAD участвуют поля *Frame Control, Address 1, Address 2, Address 3, Sequence Control, QoS Control*. Алгоритм CCM обеспечивает целостность полей, включенных в AAD;

3) из PN, поля приоритета и поля *Address 2* заголовка оригинального кадра формируется *nonce*;

4) новый PN и идентификатор ключа помещаются в 8-октетный заголовок кадра CCMP;

5) временный ключ, AAD, *nonce* и данные используются для получения шифрованного текста и MIC. Сначала, используя AES CCM в режиме CBC-MAC, вычисляется MIC, который добавляется к полю данных кадра и позволяет проверить целостность сообщения. Далее, используя AES CCM в режиме CTR, выполняется шифрование данных и MIC;

6) из заголовка оригинального кадра, заголовка CCMP, шифрованных данных и MIC в блоке II формируется шифрованный кадр CCMP (рис. 4.7), который передается по сети.

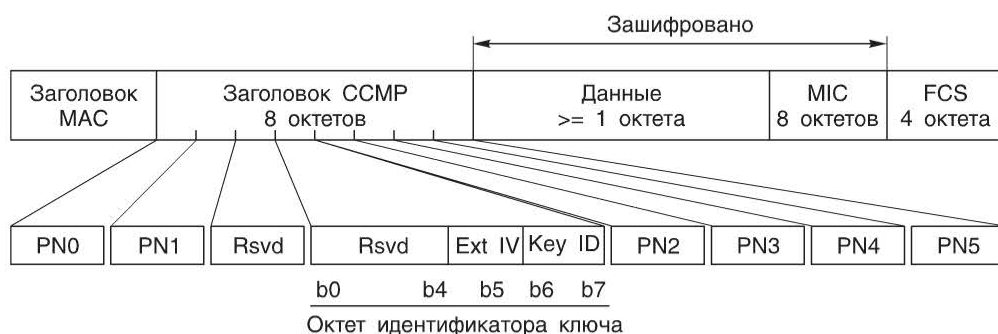


Рис. 4.7. Формат кадра CCMP

Процесс дешифрования кадра состоит из следующих шагов (рис. 4.8):

1) шифрованный кадр CCMP анализируется с целью получения значений AAD и *nonce*;

2) AAD формируется из заголовка шифрованного кадра CCMP;

3) значение *nonce* формируется из PN, поля приоритета и поля *Address 2* (A2 на рис. 4.8);

4) из кадра извлекается значение MIC с целью последующей проверки целостности сообщения;

5) выполняется дешифрование данных, для чего на вход алгоритма CCM подается временный ключ, AAD, *nonce*, MIC и зашифрованные данные. Выполняется проверка целостности данных и соответствующих полей заголовка оригинального кадра, защищенных AAD;

6) в случае успешной проверки целостности полученные из кадра CCMP заголовок и открытые данные объединяются в блоке II, и формируется оригинальный кадр;

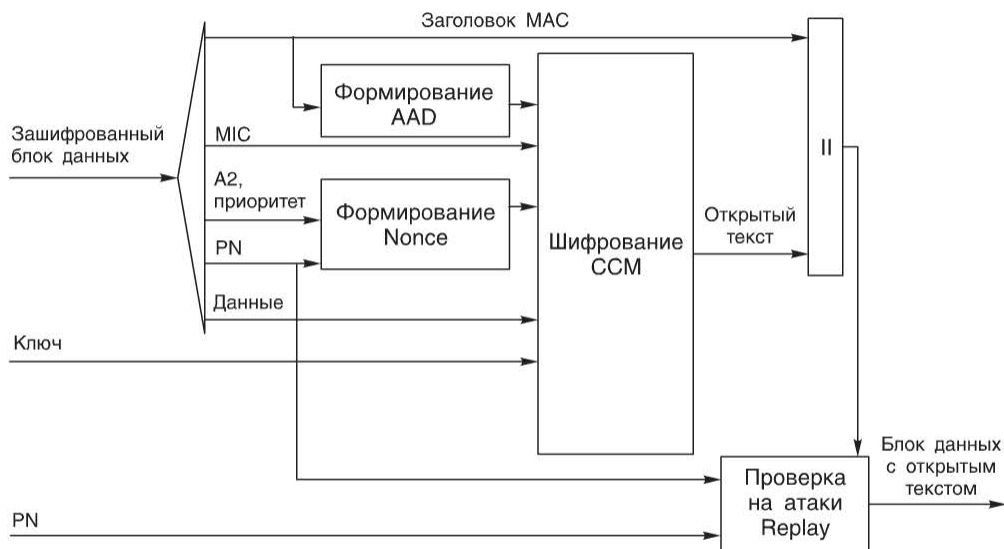


Рис. 4.8. Процесс дешифрования кадра CCMP

7) процесс дешифрования предотвращает атаки типа *replay*, проверяя значение PN;

8) если процесс проверки на атаки типа *replay* прошел успешно, кадр обрабатывается получателем.

4.4. Программы сертификации WPA/WPA2

Безопасность беспроводных сетей является весьма важным вопросом, поэтому в 2000 году Wi-Fi Alliance запустил программу сертификации, определяющую требования к безопасности беспроводных сетей, включая поддержку WEP. Быстрое развитие беспроводных технологий, а также уязвимость WEP привели к необходимости разработки новых механизмов защиты. В дополнение к функциям безопасности, существовавшим в оригинальном стандарте IEEE 802.11, рабочая группа IEEE 802.11i разработала набор расширенных функций безопасности. Для того чтобы ускорить их внедрение в беспроводных сетях, в 2003 году Wi-Fi Alliance представил программу сертификации Wi-Fi Protected Access (WPA). Она основывалась на проекте стандарта IEEE 802.11i и представляла собой набор механизмов безопасности, которые позволяли решить большинство проблем с обеспечением защиты сетей 802.11. Вместо протокола WEP в WPA использовался протокол TKIP. Также WPA включала поддержку проверки целостности сообщений. Аутентификация выполнялась на основе протокола IEEE 802.1X с EAP для корпоративных пользователей и на основе PSK для домашних пользователей и пользователей небольших офисов.

4. Безопасность передачи данных в беспроводных сетях

В 2004 году стандарт IEEE 802.11i был ратифицирован. Параллельно Wi-Fi Alliance представил программу сертификации WPA2, основанную на WPA, но вместо протокола TKIP использующую более криптоустойчивый протокол шифрования CCMP. Аутентификация так же, как и в WPA, выполняется на основе протоколов IEEE 802.1X с EAP или PSK. Изначально WPA2 была дополнительной программой сертификации, но начиная с 2006 года соответствие требованиям WPA2 является обязательным для всех устройств Wi-Fi Certified. Следует отметить, что WPA2 позволяет защитить не только кадры данных, но и кадры управления. В табл. 4.1 приведено сравнение функциональности WEP, WPA, WPA2.

Таблица 4.1. Функциональность WEP, WPA, WPA2

	WEP	WPA	WPA2
Протокол шифрования	Алгоритм RC4 с ручным назначением ключей	Протокол TKIP, основанный на RC4	Протокол CCMP с ключами AES длиной 128 бит
Целостность данных	Линейная хэш-функция	Криптографическая хэш-функция	
Управление ключами	Нет	Да	
Обнаружение атак типа <i>replay</i>	Нет	Да	

Таблица 4.2. Возможности беспроводных сетей, работающих в режимах WPA/WPA2-Personal и WPA/WPA2-Enterprise

WPA/WPA2-Personal	WPA/WPA2-Enterprise
Централизованно неуправляемый режим аутентификации на основе PSK (используется вводимая вручную парольная фраза, общая для всех пользователей сети)	Каждому пользователю назначаются индивидуальные права доступа после IEEE 802.1X-аутентификации
Не требуется сервер аутентификации	Требуется сервер аутентификации IEEE 802.1X AAA с поддержкой EAP и база аутентификационных данных
Ключи шифрования данных уникальны для каждой сессии	

В зависимости от требований сети WPA/WPA2 могут работать в одном из двух режимов — Enterprise и Personal. Поддержка режима WPA/WPA2-Personal является обязательной для всех сертифицированных Wi-Fi Alliance точек доступа и беспроводных адаптеров. Поддержка режима WPA/WPA2-

Enterprise является опциональной, но рекомендованной для устройств, работающих в больших корпоративных сетях.

Сравнение возможностей беспроводных сетей, работающих в режимах WPA/WPA2-Personal и WPA/WPA2-Enterprise, приведено в табл. 4.2.

В домашних сетях и сетях небольших офисов обычно используется режим WPA/WPA2-Personal, поскольку в этом случае не требуется никакого дополнительного оборудования, кроме точки доступа и клиентского устройства. Ключ PSK в режиме WPA/WPA2-Personal получают из SSID и парольной фразы, указанной в настройках устройства (рис. 4.9). Для повышения безопасности сетей рекомендуется использовать сложные парольные фразы и как можно чаще обновлять их. Режим WPA/WPA2-Enterprise предназначен для корпоративных сетей, в которых используются серверы аутентификации IEEE 802.1X (рис. 4.10). Этот режим включает возможность мониторинга и управления трафиком, определения прав доступа пользователей, включая предоставление гостевого доступа.

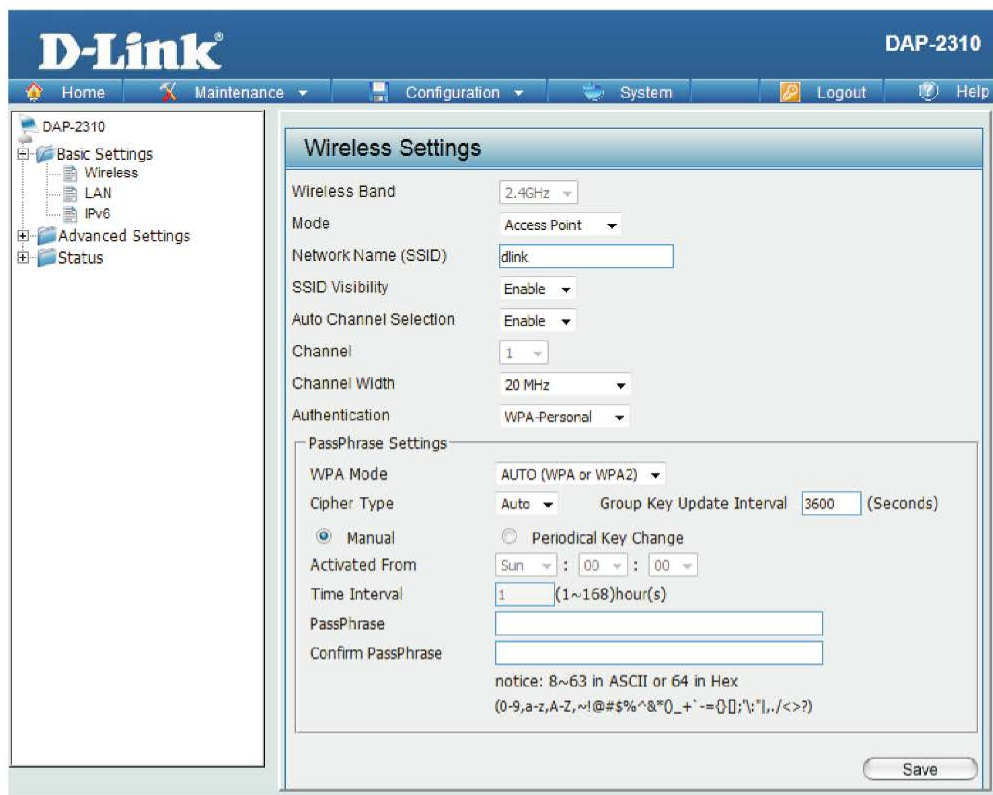


Рис. 4.9. Настройка режима WPA/WPA2-Personal на точке доступа D-Link DAP-2310

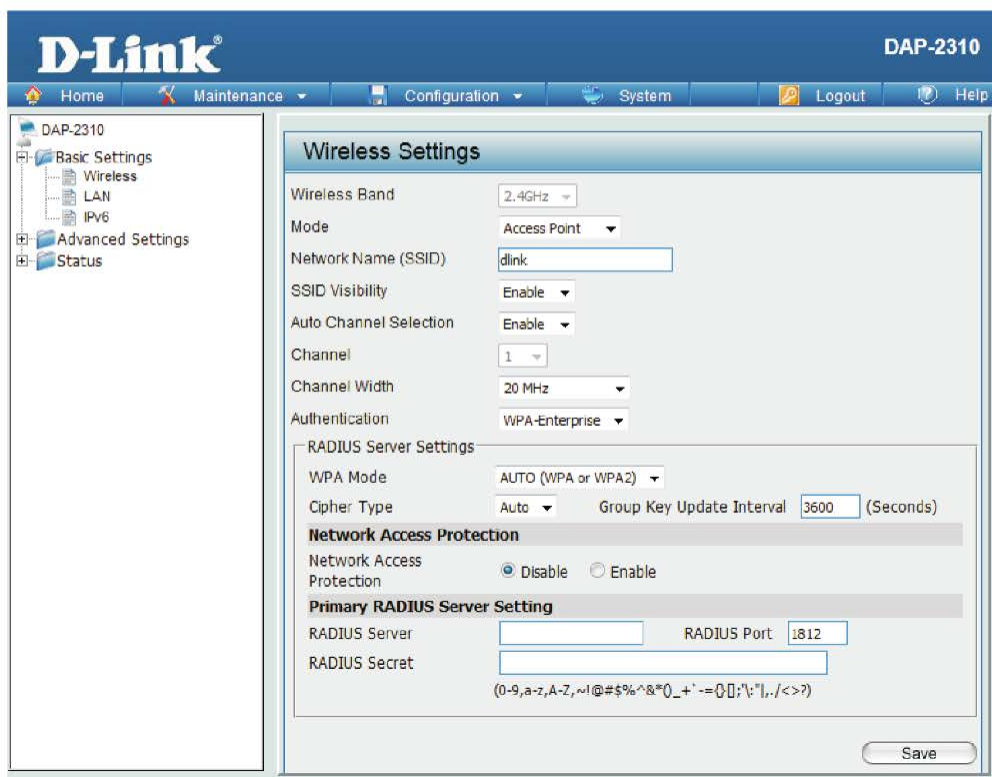


Рис. 4.10. Настройка режима WPA/WPA2-Enterprise на точке доступа D-Link DAP-2310

4.5. Программа сертификации Wi-Fi Protected Setup (WPS)

Для упрощения настройки возможностей WPA2 в домашних сетях и сетях небольших офисов в 2007 году Wi-Fi Alliance представил дополнительную программу сертификации Wi-Fi Protected Setup (WPS). WPS является методом автоматической настройки параметров WPA2 (в режиме WPA2-Personal) на беспроводных устройствах, предназначенных для рынка SOHO. Устройство, поддерживающее WPS, должно быть маркировано знаком, показанным на рис. 4.11. Пользователям таких устройств не требуется вводить парольную фразу и SSID, поскольку WPS выполняет все настройки безопасности автоматически. Основной задачей WPS является обеспечение простоты подключения беспроводных устройств к сети с соблюдением всех требований безопасности и шифрования для пользователей, не обладающих знаниями в области сетевых технологий. При необходимости пользователь может выполнить все настройки WPA2 на WPS-совместимом устройстве вручную.



Рис. 4.11. Лого-тип WPS

Устройства с поддержкой WPS предлагают пользователям один из трех методов настройки WPA2:

- *Personal Identification Number (PIN)*: этот метод является обязательным для точек доступа и клиентских устройств. Для создания соединения пользователь через интерфейс настройки устройства вводит персональный идентификационный номер (PIN), который может быть указан на самом устройстве или сгенерирован динамически.

- *Push Button Configuration (PBC)*: этот метод является обязательным для точек доступа и опциональным для клиентских устройств. Используя этот метод, пользователь нажимает на кнопку WPS (физическую или виртуальную) на точке доступа и соответствующем клиентском устройстве, запуская тем самым автоматическую процедуру установления безопасного соединения.

- *Near Field Communication (NFC)*: этот метод является опциональным. Пользователь при этом использует NFC-токен или физически соединяет точку доступа с клиентским устройством (по аналогии соединения компьютера с фотоаппаратом для передачи фотоизображения).

Рассмотрим пример создания защищенного соединения между клиентом с установленным беспроводным адаптером D-Link DWA-160 и маршрутизатором D-Link DIR-860L, используя метод PIN.

Шаг 1. Установить и запустить на клиентском устройстве утилиту D-Link Connection Manager для DWA-160. В открывшемся окне нажать кнопку *WPS* (рис. 4.12).

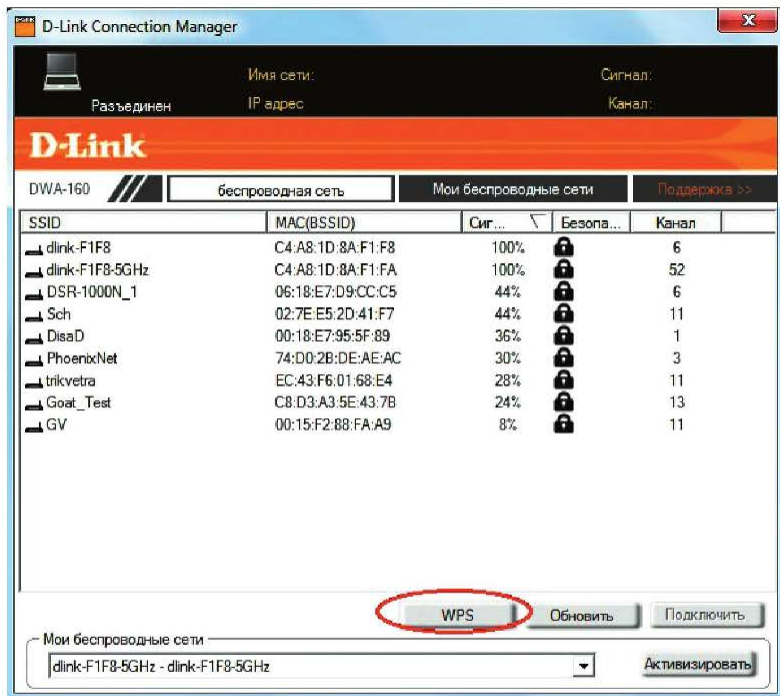


Рис. 4.12. Интерфейс утилиты D-Link Connection Manager

Шаг 2. В появившемся окне выбрать функцию *PIN* (персональный идентификационный номер) и нажать кнопку *Далее* (рис. 4.13).

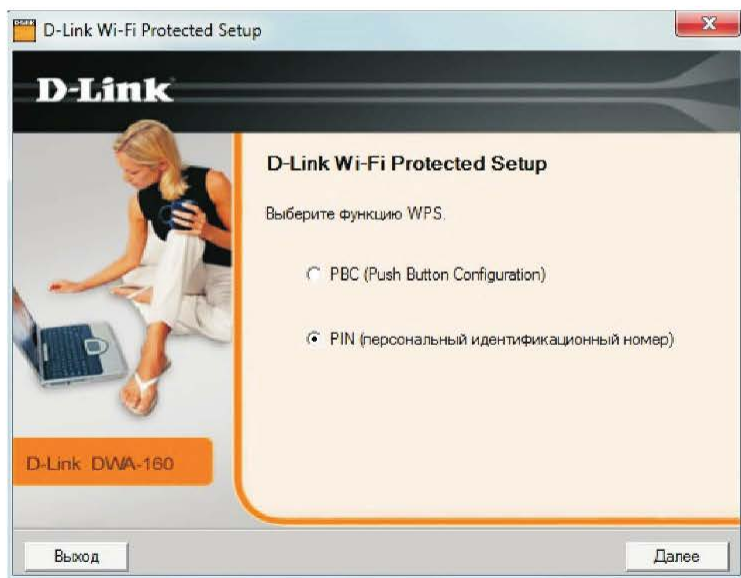


Рис. 4.13. Выбор метода PIN

Шаг 3. Автоматически сгенерируется PIN, который необходимо ввести в интерфейсе настройки маршрутизатора DIR-860L (рис. 4.14).

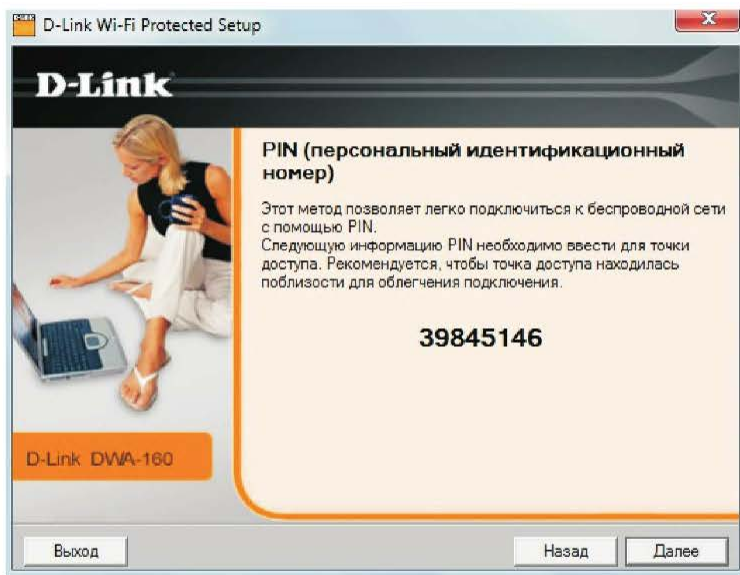


Рис. 4.14. Сгенерированный PIN

Шаг 4. На маршрутизаторе зайти на Web-интерфейс, перейти во вкладку *Setup* → *Wireless Settings* → *Add Wireless Device with WPS* (рис. 4.15).

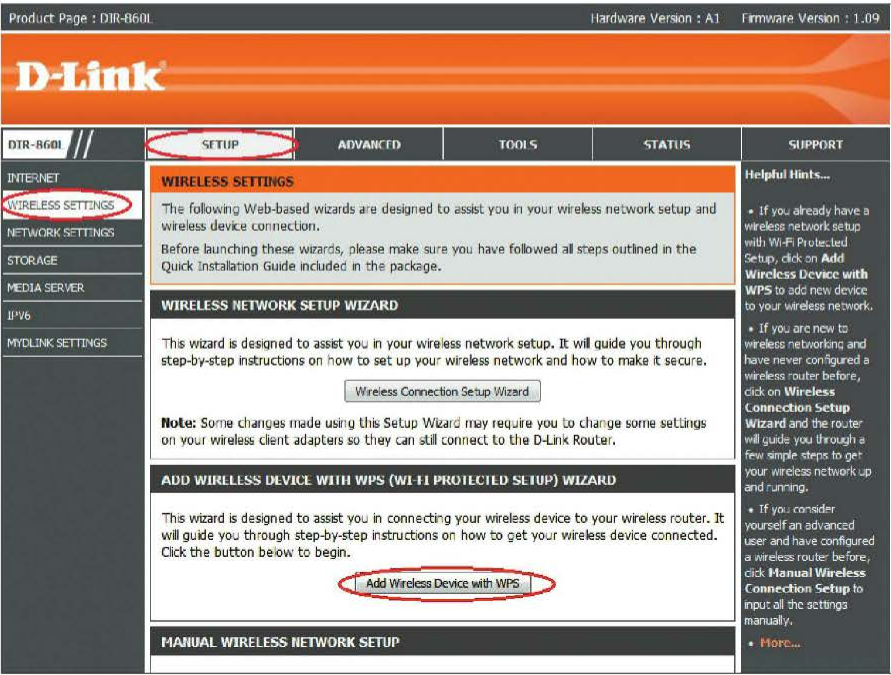


Рис. 4.15. Web-интерфейс маршрутизатора D-Link DIR-860L

Шаг 5. В открывшемся окне установить переключатель *Auto* и нажать кнопку *Next* (рис. 4.16).

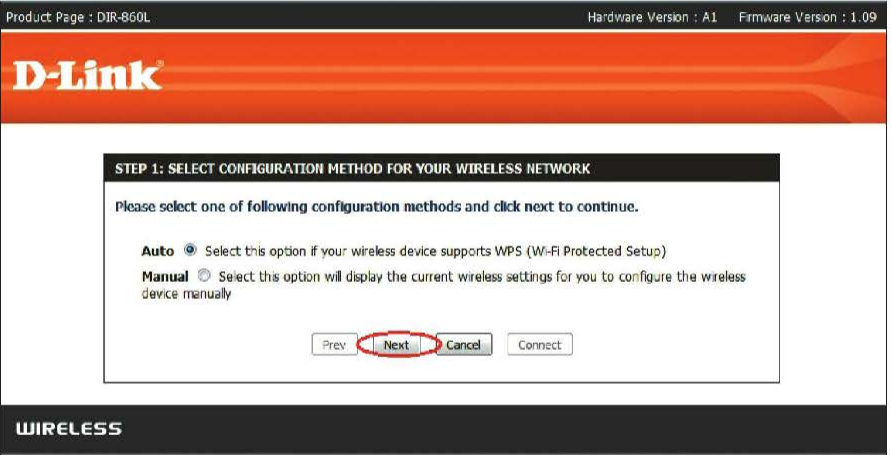


Рис. 4.16. Выбор способа подключения к беспроводной сети

4. Безопасность передачи данных в беспроводных сетях

Шаг 6. В появившемся окне выбрать *PIN*, ввести идентификационный номер, сгенерированный утилитой D-Link Connection Manager на шаге 3, и нажать кнопку *Connect* (рис. 4.17). При этом запустится процедура установления защищенного беспроводного соединения.

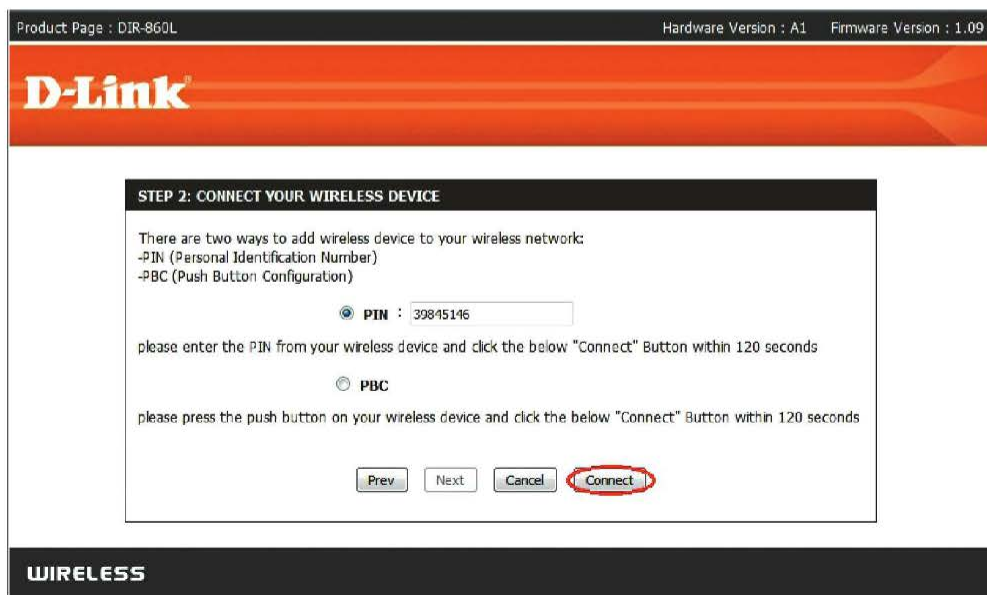


Рис. 4.17. Выбор метода WPS и ввод PIN

Для установления защищенного беспроводного соединения методом PBC необходимо одновременно нажать кнопки WPS, расположенные на корпусе беспроводного адаптера и маршрутизатора (рис. 4.18).



Рис. 4.18. Установление защищенного беспроводного соединения с помощью метода PBC

5. Физический уровень стандарта IEEE 802.11

Физический уровень стандарта IEEE 802.11 состоит из двух подуровней (рис. 5.1):

- *Physical Layer Convergence Procedure (PLCP)* — процедура конвергенции физического уровня. Этот подуровень управляет обменом кадров между

Канальный уровень	Подуровень MAC
Физический уровень	PLCP
	PMD

Рис. 5.1. Архитектура физического уровня 802.11

MAC-подуровнем и физическим уровнем. PLCP позволяет двум и более беспроводным станциям передавать и принимать данные, используя подуровень PMD. PLCP формирует кадр соответствующего подуровня PMD из блока данных подуровня MAC, преамбулы и заголовка физического уровня;

- *Physical Medium Dependent (PMD)* — подуровень зависимости от физической среды. Этот подуровень обеспечивает интерфейс со средой

передачи данных. Он определяет характеристики беспроводной среды и метод передачи данных беспроводными станциями через нее.

Другими словами, подуровень PLCP является связующим звеном между MAC-подуровнем и средой передачи. Он формирует кадр, передаваемый подуровнем PMD через беспроводную среду с помощью антенн.

Также физический уровень включает в себя функцию *Clear Channel Assessment (CCA)*, которая определяет текущее состояние использования среды передачи и позволяет MAC-подуровню контролировать несущую.

В оригинальном стандарте IEEE 802.11, появившемся в 1997 году, определены три протокола физического уровня (*Physical Layer Protocol, PHY*):

- передача в диапазоне инфракрасных волн (*Infrared (IR) PHY*);
- расширение спектра методом скачкообразной перестройки частоты в диапазоне 2,4 ГГц (*FHSS PHY*);
- расширение спектра методом прямой последовательности в диапазоне 2,4 ГГц (*DSSS PHY*).

Эти технологии позволяют выполнять передачу данных на скоростях 1 и 2 Мбит/с. В 1999 году были разработаны еще два протокола физического уровня:

- 802.11a — мультиплексирование с ортогональным частотным разделением (*Orthogonal Frequency Division Multiplexing, OFDM PHY*);
- 802.11b — расширение спектра методом прямой последовательности с элементарным кодированием (*High Rate (HR) / DSSS PHY*).

Спецификация 802.11a является первой спецификацией физического уровня, которая использует для передачи полосу частот 5 ГГц и определяет скорости передачи до 54 Мбит/с. К ее достоинствам можно отнести меньшую интерференцию (так как используется менее загруженный диапазон 5 ГГц).

Однако эффективный радиус действия сетей 802.11a меньше по сравнению с сетями, работающими на частоте 2,4 ГГц, поскольку радиоволны в диапазоне 5 ГГц ослабевают сильнее, чем на 2,4 ГГц.

Спецификация 802.11b, появившаяся позже спецификации 802.11a, основана на расширении физического уровня DSSS, обеспечив скорости передачи 5,5 и 11 Мбит/с в диапазоне 2,4 ГГц. Радиус действия у сетей 802.11b больше, чем у сетей 802.11a, но из-за использования частоты 2,4 ГГц, на которой работает множество бытовых устройств, включая микроволновые печи, радиотелефоны и т.д., сети 802.11b сильнее подвержены интерференции.

В 2003 году появилась спецификация 802.11g, объединяющая в себе сильные стороны двух предыдущих (802.11a и 802.11b) спецификаций. Она использует диапазон 2,4 ГГц и позволяет передавать данные на скорости до 54 Мбит/с. Спецификации 802.11g соответствует *физический уровень с расширенной скоростью (Extended Rate Physical Layer, ERP) для систем DSSS (ERP PHY)*. Оборудование спецификации 802.11g обратно совместимо с оборудованием спецификации 802.11b.

Следующей спецификацией физического уровня стала 802.11n, появившаяся в 2009 году. Скорость передачи данных возросла до 600 Мбит/с при работе в диапазонах 2,4 и 5 ГГц. Спецификация 802.11n определяет *физический уровень с высокой производительностью (High Throughput, HT) для систем OFDM (HT PHY)*. Высокие скорости передачи достигаются в 802.11n благодаря использованию антенной технологии MIMO (Multiple Input Multiple Output), каналов шириной 40 МГц, пространственно-временных блочных кодов и агрегации кадров на MAC-подуровне. Оборудование спецификации 802.11n обратно совместимо с оборудованием спецификации 802.11a при работе в диапазоне 5 ГГц и 802.11b/g при работе в диапазоне 2,4 ГГц.

В 2013 году появилась спецификации 802.11ac, позволяющая приблизить скорости беспроводных устройств к скоростям проводного оборудования. Она определяет еще один физический уровень: *физический уровень с очень высокой производительностью (Very High Throughput, VHT) для систем OFDM (VHT PHY)*. Спецификация 802.11ac определяет скорости передачи до 6,93 Гбит/с и поддерживает работу только в диапазоне 5 ГГц. Оборудование спецификации 802.11ac обратно совместимо с оборудованием спецификаций 802.11a и 802.11n.

В 2012 году все появившиеся до этого момента дополнения оригинального стандарта 802.11, включая 802.11a, 802.11b, 802.11g, 802.11n, были объединены в один документ IEEE 802.11–2012. Спецификация 802.11ac описана в стандарте IEEE 802.11ac–2013. В табл. 5.1 приведены технические характеристики рассмотренных выше спецификаций физического уровня 802.11.

Внимание: устройства спецификации 802.11, работающие в одном частотном диапазоне, обратно совместимы друг с другом. Если в техническом описании устройства указано «поддержка IEEE 802.11b/g/n» — это означает, что данное устройство соответствует спецификации 802.11n и способно работать в диапазоне частот 2,4 ГГц с устройствами спецификаций 802.11b и 802.11g на максимальных для них скоростях: 11 Мбит/с и 54 Мбит/с соответственно.

Таблица 5.1. Спецификации физического уровня 802.11

Характеристики	Спецификации				
	802.11a	802.11b	802.11g	802.11n	802.11ac
Стандарт принят	Сентябрь 1999	Сентябрь 1999	Июль 2003	Сентябрь 2009	Январь 2014
Скорость передачи, Мбит/с	До 54	До 11	До 54	До 600	До 6933
Диапазон частот, ГГц	5	2,4	2,4	2,4 и 5	5
Ширина канала, МГц	20	22	20 или 22	20 или 40	20, 40, 80, 160 или 80+80
Тип модуляции	OFDM	DSSS, CCK	DSSS, CCK, OFDM	DSSS, CCK, OFDM	OFDM
Антенная технология	SISO	SISO	SISO	MIMO	MIMO/ MU-MIMO
Количество пространственных потоков	1	1	1	От 1 до 4	От 1 до 8

5.1. Особенности использования радиочастотного спектра

Порядок и правила использования радиочастотного спектра определяются государством. В России роль регулятора выполняет Государственная комиссия по радиочастотам (ГКРЧ). В США за регулирование спектра отвечает Federal Communications Commission (FCC), в Европе — CEPT's European Radiocommunications Office (ERO) и European Telecommunications Standards Institute (Европейский институт по стандартизации в области телекоммуникаций, ETSI). Правила использования радиочастотного спектра необходимы для того, чтобы множество беспроводных устройств могло одновременно использовать одну полосу частот, не создавая помех друг другу. Во многих случаях пользователи или операторы связи должны получать разрешительные документы на использование частот. Этими документами ограничена рабочая частота, выходная мощность передатчика и область распространения беспроводного сигнала.

Весь радиоспектр разделен на частотные диапазоны, предназначенные для конкретных целей. В России для беспроводных сетей стандарта 802.11

выделены одна полоса в диапазоне 2,4 ГГц (2400–2483,5 МГц) и две полосы в диапазоне 5 ГГц (5150–5350 МГц и 5650–6425 МГц).

Внимание: границы частотных диапазонов для использования устройствами Wi-Fi в разных странах могут отличаться. Особенности использования того или иного частотного диапазона в России определяются законодательными актами ГРЧ.

Частотные диапазоны 2,4 и 5 ГГц, в свою очередь, разбиваются на каналы, ширина и количество которых зависит от спецификации 802.11 и особенностей радиочастотного регулирования в конкретном государстве.

Ширина частотных каналов спецификации 802.11b составляет 22 МГц, так как при этом используется физический уровень DSSS. Оборудование спецификации 802.11g также использует каналы шириной 22 МГц, хотя в литературе указывается ширина канала 802.11g, равная 20 МГц. Это утверждение правильно только отчасти: поскольку в спецификации 802.11g комбинируются методы модуляции спецификаций 802.11b (DSSS) и 802.11a (OFDM), ширина канала равна 22 и 20 МГц соответственно. Ширина канала спецификации 802.11a равна 20 МГц, в 802.11n могут использоваться каналы шириной 20 или 40 МГц, 802.11ac определяет использование каналов шириной 20, 40, 80 или 160 МГц.

В России в диапазоне 2400–2483,5 МГц доступно до 13 каналов передачи (при ширине канала 20/22 МГц), три из которых являются неперекрывающимися (табл. 5.2).

Таблица 5.2. Каналы, доступные в диапазоне 2,4 ГГц

Номер канала	Диапазон занимаемых каналом частот, МГц	Центральная частота канала, МГц
1	2401–2423	2412
2	2406–2428	2417
3	2411–2433	2422
4	2416–2438	2427
5	2421–2443	2432
6	2426–2448	2437
7	2431–2453	2442
8	2436–2458	2447
9	2441–2463	2452
10	2446–2468	2457
11	2451–2473	2462
12	2456–2478	2467
13	2461–2483	2472

Таблица 5.3. Каналы, доступные в диапазоне 5 ГГц

Номер канала	Центральная частота канала, МГц	Номер канала	Центральная частота канала, МГц
34	5170	147	5735
36	5180	149	5745
38	5190	151	5755
40	5200	153	5765
42	5210	155	5775
44	5220	157	5785
46	5230	159	5795
48	5240	161	5805
52	5260	163	5815
56	5280	165	5825
60	5300	167	5835
64	5320	171	5855
132	5660	173	5865
136	5680	177	5885
140	5700	180	5905

Частотный план для диапазона 5 ГГц организуется сложнее, чем для диапазона 2,4 ГГц, поскольку диапазон 5 ГГц не является непрерывным. Всего в частотном диапазоне 5 ГГц имеется более 20 неперекрывающихся каналов (при ширине канала 20 МГц), работа на которых возможна без взаимных помех (табл. 5.3).

5.2. Технологии модуляции физического уровня IEEE 802.11

Технологии модуляции физического уровня 802.11 определяют, каким образом и на какой скорости данные передаются через беспроводную среду. Ниже будут рассмотрены две основные технологии — расширение спектра методом прямой последовательности (DSSS) и мультиплексирование с ортогональным частотным разделением (OFDM).

5.2.1. Технологии расширения спектра

Технологии *расширения спектра* (*Spread Spectrum*) являются базовыми при организации передачи данных в беспроводных сетях стандарта 802.11. Их основная идея заключается в преобразовании информационного сигнала с узкой полосой пропускания в сигнал с широкой полосой пропускания. При этом преобразовании мощность исходного сигнала не изменяется, а распределяется по более широкой полосе пропускания и становится сопоставима с мощностью шумов. Расширение спектра обеспечивает:

- невосприимчивость сигнала к различным типам шумов, а также искажениям, вызванным его многолучевым распространением;
- возможность скрывать и шифровать сигналы;
- одновременное использование одной полосы частот несколькими пользователями с крайне малой взаимной интерференцией.

Чтобы минимизировать интерференцию между беспроводными устройствами, регуляторы ограничивают мощность передатчиков беспроводного оборудования и максимальную эффективную изотропно-излучаемую мощность (ЭИИМ).

Физические уровни IEEE 802.11 используют два метода расширения спектра в диапазоне 2,4 ГГц:

- метод скачкообразной перестройки частоты (FHSS);
- метод прямой последовательности (DSSS).

При расширении спектра *методом скачкообразной перестройки частоты* (*Frequency-Hopping Spread Spectrum, FHSS*) передача сигнала производится с помощью наборов частот, имеющих свойства случайных последовательностей (рис. 5.2). Перестройка частоты сигнала происходит через определенные интервалы времени, поэтому для получения сигнала требуется синхронизация изменений рабочих частот приемника и передатчика. Физический уровень FHSS стандарта 802.11 позволяет выполнять передачу данных на скоростях 1 и 2 Мбит/с. В качестве схемы модуляции для скорости 1 Мбит/с используется двухуровневая гауссова частотная манипуляция (GFSK): двоичные нуль и единица кодируются как отклонение от текущей несущей частоты. Для скорости 2 Мбит/с используется четырехуровневая GFSK, в которой четыре различных отклонения от несущей представляют четыре двухбитовые комбинации нулей и единиц.

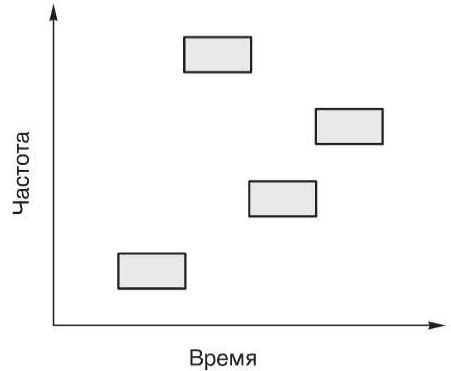


Рис. 5.2. Перестройка частоты

Расширение спектра *методом прямой последовательности* (*Direct Sequence Spread Spectrum, DSSS*) лучше приспособлено для передачи данных на высоких скоростях, чем FHSS. Также этот метод больше устойчив к интерференции сигналов.

Физический уровень DSSS используется в спецификациях 802.11b и 802.11g. Его основным принципом является распределение мощности сигнала по широкому частотному диапазону. Для этого исходный сигнал модулируется расширяющей последовательностью. Для расширения спектра сигнала в стандарте 802.11 определено использование *последовательности Баркера* (*Barker sequence*), обладающей наилучшими среди известных псевдослучайных последовательностей свойствами шумоподобности. Длина ис-

пользуемой в 802.11 последовательности — 11 чипов (+1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1). При использовании в 802.11 «+1» становится двоичной единицей, а «-1» становится двоичным нулем, поэтому в двоичном виде последовательность представляется как 10110111000.

Передатчик заменяет каждый бит исходного потока данных на кодовую последовательность длиной 11 бит с помощью операции XOR. Таким образом, каждая двоичная единица исходного потока данных отображается в последовательность 01001000111, а каждый двоичный ноль — в последовательность 10110111000 (рис. 5.3). Далее полученная последовательность из 11 бит модулируется и передается в общий канал.

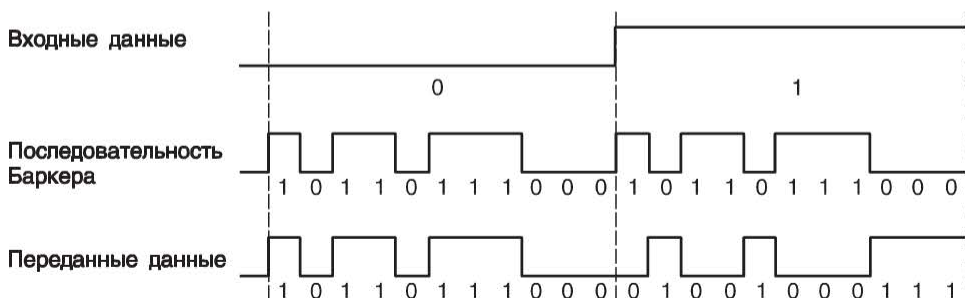


Рис. 5.3. Кодирование с помощью последовательности Баркера

В качестве схемы модуляции для скорости 1 Мбит/с используется *дифференциальная двухуровневая фазовая манипуляция (DBPSK)* (рис. 5.4): при передаче двоичного нуля фаза несущего сигнала не изменяется, при передаче двоичной единицы фаза несущего сигнала меняется на 180°.

В качестве схемы модуляции для скорости 2 Мбит/с применяется *дифференциальная квадратурная фазовая манипуляция (DQPSK)*: используются четыре значения фазы несущего сигнала (0, 90°, 180°, 270°), каждое состояние фазы выполняет передачу сразу двух бит последовательности (00, 01, 10, 11). Изменение фазы происходит при изменении информационных битов.

Приемник после получения сигнала демодулирует его с использованием той же чиповой последовательности. Далее исходный информационный сигнал восстанавливается и становится узкополосным.

По причине избыточности, вносимой DSSS, мощность исходного сигнала может быть достаточно небольшой. При этом значительно снижается отношение уровня мощности передаваемого сигнала к уровню мощности шума. Благодаря очень низкому уровню мощности сигнала устройства DSSS практически не создают помех обычным радиоустройствам (узкополосным большой мощности), так как для них широкополосный сигнал выглядит как шум в пределах допустимого. И наоборот — обычные устройства не мешают широкополосным, так как их сигналы большой мощности создают шум только в своем узком диапазоне и не могут целиком заглушить весь широкополосный сигнал.

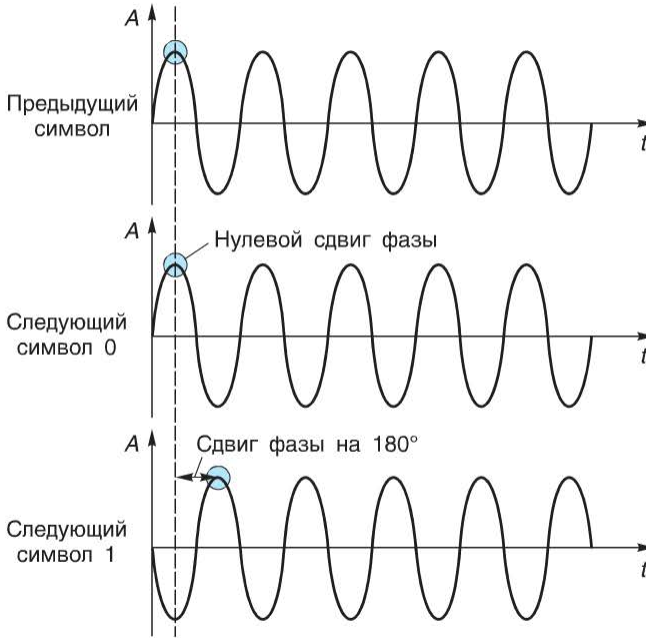


Рис. 5.4. Модуляция DBPSK

Ширина канала физического уровня DSSS равна 22 МГц. В России в диапазоне 2400–2483,5 МГц для устройств с физическим уровнем DSSS доступно до 13 каналов. Центральная частота первого канала 2412 МГц, второго — 2417 МГц, третьего — 2422 МГц и т. д. (рис. 5.5). Каждый последующий канал смещен относительно центра предыдущего на 5 МГц и не перекрывается с предыдущим на 5 МГц.

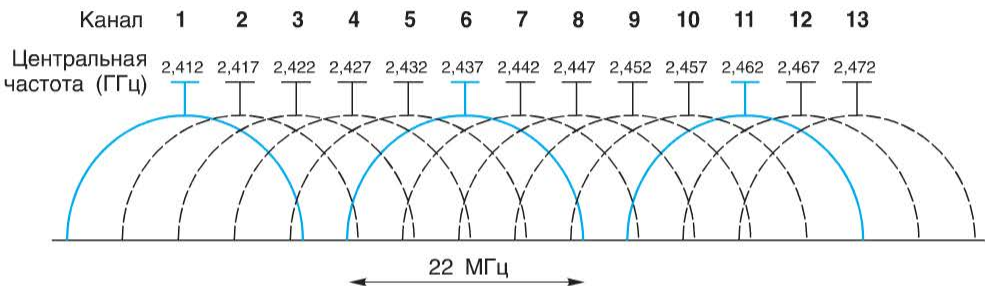


Рис. 5.5. Каналы, используемые в технологии DSSS

Для каждого физического уровня стандарт 802.11 определяет *спектральные маски* (*spectral mask*) излучаемых сигналов, которые устанавливают распределение энергии внутри канала. Спектральная маска требует затухания сигнала на определенных уровнях, смещенных относительно центральной частоты, чтобы избежать интерференции с соседними каналами.

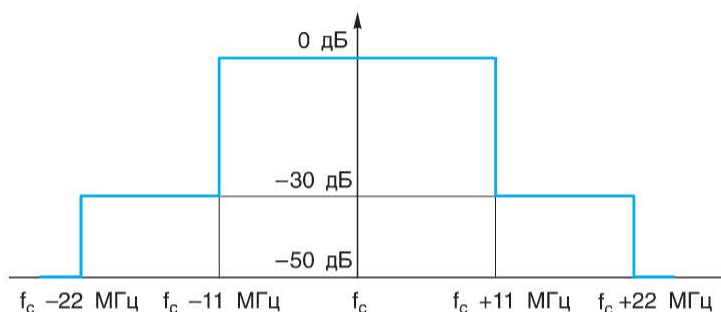


Рис. 5.6. Спектральная маска сигнала спецификации 802.11b

На рис. 5.6 показана спектральная маска сигнала спецификации 802.11b с физическим уровнем DSSS. Основная часть энергии спектра распределяется по каналу шириной 22 МГц. Полностью же спектр занимает более широкую полосу частот и должен затухать не меньше чем на 30 дБ (ослабляться в 1000 раз) на расстоянии 11 МГц от центра канала. На рис. 5.7 показаны спектральная маска и спектр реального сигнала спецификации 802.11b с физическим уровнем DSSS в канале шириной 22 МГц. Данное изображение было получено с помощью векторного частотного анализатора сигналов, входящего в состав тестового оборудования компании D-Link.



Рис. 5.7. Спектральная маска и спектр реального сигнала спецификации 802.11b DSSS

Регуляторы ограничивают мощность передатчиков, чтобы оборудование не создавало помех устройствам, работающим на соседних каналах, в том числе неперекрывающихся. В России при использовании устройств внутри помещений их излучаемая мощность ограничена 100 мВт.

Оборудование с физическим уровнем DSSS может быть настроено для работы на любом из 13 каналов. Соседние сети, т. е. сети, находящиеся в одной зоне покрытия, для устранения взаимной интерференции должны использовать каналы, центральные частоты которых отстоят друг от друга не менее чем на 25 МГц. Другими словами, разница между номерами каналов соседних сетей должна быть равна 5. В диапазоне 2,4 ГГц существует три неперекрывающихся канала с номерами 1, 6, 11.

5.2.2. Мультиплексирование с ортогональным частотным разделением

При мультиплексировании с ортогональным частотным разделением (*Orthogonal Frequency Division Multiplexing, OFDM*) вся полоса пропускания канала разделена на множество поднесущих (*subcarrier*) или вспомогательных несущих. Число этих поднесущих может быть сколь угодно большим, в стандарте 802.11 используются от 52 до 484 поднесущих. Число поднесущих зависит от режима работы и ширины частотного канала. Некоторые из поднесущих являются вспомогательными (пилотными) и используются для синхронизации передачи и декодирования данных по основным (информационным) несущим.

Формируемые поднесущие являются ортогональными, а значит, передача информации на каждой из них не влияет на передачу информации на соседних. Это вытекает из того, что математически ортогональность означает равенство нулю скалярных произведений сигналов разных поднесущих, т. е. если при передаче одна из поднесущих сместится по частоте и займет место другой поднесущей, то при демодуляции OFDM-символа в приемнике сигнал на последней будет равен нулю, что показывает отсутствие межканальной интерференции таких сигналов.

Физически ортогональность несущих сигналов обеспечивается, когда за время длительности одного символа несущий сигнал будет совершать целое число колебаний.

Как показано на рис. 5.8, центры поднесущих размещены так, что максимум энергии одной поднесущей совпадает с минимумами других поднесущих, несмотря на то, что их сигналы частично пересекаются в частотном спектре. Такое размещение позволяет более эффективно использовать доступную полосу частот.

Внимание: мультиплексирование с ортогональным частотным разделением также называют модуляцией с множеством несущих.

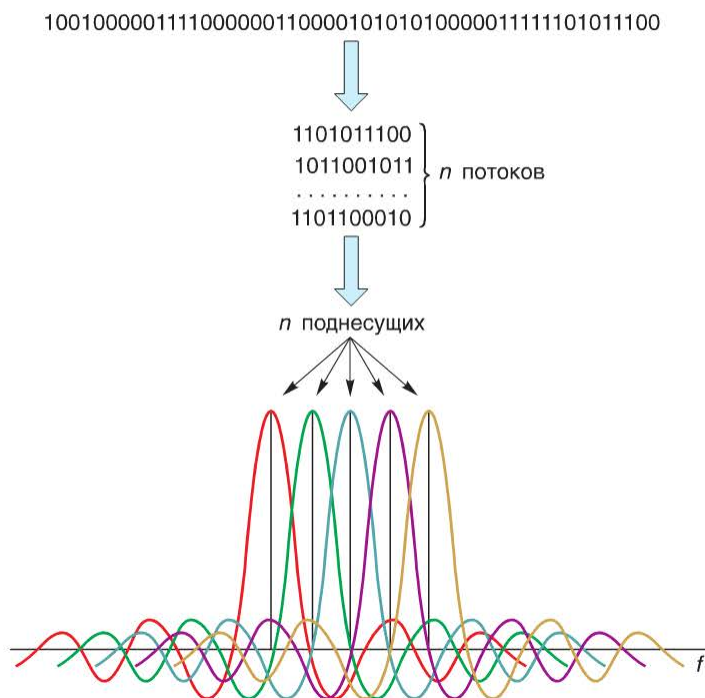


Рис. 5.8. Мультиплексирование с ортогональным частотным разделением

Передача данных ведется одновременно всеми поднесущими. Исходящий высокоскоростной поток данных разбивается в передатчике на n низкоскоростных потоков $x[n]$ (n — число поднесущих), каждый из которых модулируется своей отдельной поднесущей с помощью обратного быстрого преобразования Фурье (ОБПФ), переводящего предварительно мультиплексированный на каждой поднесущей сигнал из частотного представления во временное. Суть этого преобразования сводится к умножению информационных сигналов $x[n]$ на соответствующие поднесущие и объединению их в один сигнал (рис. 5.9, а). Такое преобразование позволяет вместо широкополосного сигнала получить набор узкополосных сигналов, составляющих так называемый OFDM-символ (рис. 5.9, б). Достоинством такого преобразования является то, что при наличии узкополосной помехи будет искажена одна или несколько поднесущих, а не весь сигнал в целом, что существенно уменьшит количество ошибок, получаемых на выходе приемника (декодера). Далее этот сигнал переносится на несущую частоту и излучается антенной устройства. Вид передаваемого OFDM-сигнала во времени показан на рис. 5.9, в. В общем случае он состоит из суммы периодических функций разной частоты, число которых равно числу поднесущих. В приемнике OFDM-сигнал дополнительно искажается шумами приемных каскадов

и помехами радиоэфира и представляет собой совокупность синусоид, меняющихся во времени сложным и случайным образом. Искажения изменяют форму спектра, ослабляя сигнал на некоторых поднесущих, что приводит к ошибкам демодуляции сигнала (рис. 5.9, *г*). Успех демодуляции зависит от величины этого ослабления.

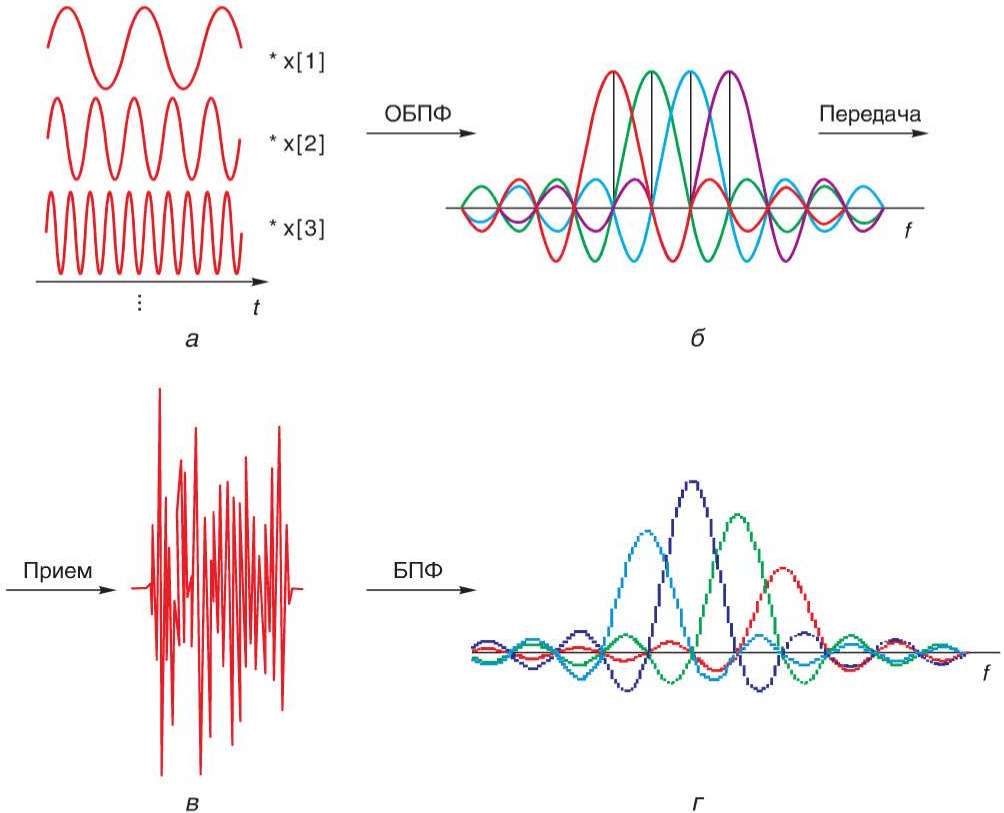


Рис. 5.9. Передача OFDM-символа

При приеме после устранения несущей радиочастоты над сигналом выполняется быстрое преобразование Фурье (БПФ), при котором все поднесущие извлекаются одновременно. Далее каждая из них подается на демодуляторы, на выходе каждого из которых выделяется n -й поток битов данных.

В отличие от уже рассмотренных физических уровней OFDM позволяет бороться с негативными последствиями многолучевого распространения. Напомним, что многолучевое распространение сигнала возникает в результате его отражения, дифракции и рассеяния. Это приводит к появлению нескольких копий сигнала, которые поступают на приемник разными путями и в разные моменты времени. Одним из эффектов многолучевого распространения является межсимвольная интерференция (ISI), возникающая, когда задержка распространения между исходным и отраженными сигналами

сравнима или больше длительности одного символа. Запоздалые отраженные сигналы предыдущего символа могут приниматься одновременно с базовым сигналом следующего символа. В результате интерференции складываются сигналы, представляющие разные биты, что приводит к повреждению данных. Межсимвольная интерференция оказывает значительное влияние на форму получаемого сигнала при высоких скоростях передачи ввиду малости расстояния между символами.

Для борьбы с межсимвольной интерференцией и интерференцией между поднесущими (возникает в результате сдвига центра поднесущей частоты)

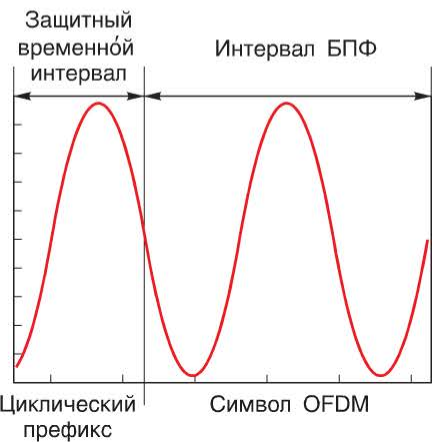


Рис. 5.10. Структура символа в OFDM на одной поднесущей с добавлением префикса

в OFDM используется *защитный* или *охраняемый интервал* (*Guard Interval, GI*). Обычно в качестве защитного интервала используют так называемый *циклический префикс*, представляющий собой циклическое повторение окончания OFDM-символа (рис. 5.10). Он добавляется перед передаваемым OFDM-символом в передатчике и удаляется при приеме символа в приемнике. Наличие защитного интервала создаст временные паузы между отдельными символами, и если его длительность превышает максимальное время задержки сигнала в результате многолучевого распространения, то межсимвольной интерференции не возникает (рис. 5.11).

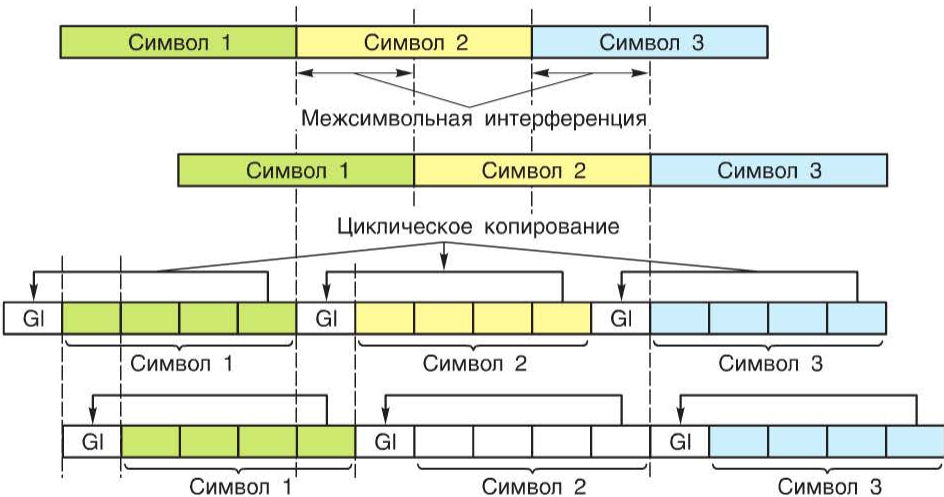


Рис. 5.11. Защитный интервал и межсимвольная интерференция

При этом защитный интервал большой длительности снижает скорость передачи данных, что усложняет задачу выбора оптимальной длительности защитного интервала.

Вследствие многократных отражений, а также наличия шумов и других радиочастотных помех передаваемые сигналы искажаются и их демодуляция приводит к возникновению ошибок в принимаемых битах, что, в свою очередь, требует повторной передачи данных и снижает общую пропускную способность канала передачи. Для исправления ошибок и поддержания максимальной пропускной способности канала используются коды с коррекцией ошибок, называемые также схемами *прямого исправления ошибок* (*Forward Error Correction, FEC*). Одной из форм кодов с коррекцией ошибок являются *сверточные коды* (*convolution coding*). OFDM использует сверточные коды на всех поднесущих, что позволяет обнаруживать и исправлять ошибки, не прибегая к повторной передаче данных. Для этого передатчик преобразует каждый k -битовый блок данных в n -битовый выходной блок ($n > k$), что повышает помехоустойчивость за счет избыточности. Сверточные коды являются кодами с памятью, поэтому выходная n -битовая последовательность для каждого k -битового блока данных зависит не только от содержимого этого блока, но и от нескольких последних k -битовых блоков.

Сверточные коды зачастую характеризуются *скоростью их кодирования* (*code rate*), которая определяется как отношение числа битов данных к общему числу бит k/n и показывает, какая доля кода приходится на полезную информацию. Сверточный код со скоростью кодирования $1/2$ указывает на то, что на один входной бит приходится два выходных. Чем меньше скорость кодирования, тем больше бит доступно для коррекции ошибок и надежнее код. Однако это приводит к снижению скорости передачи данных. Чем выше скорость кодирования, тем больше скорость передачи данных, но и выше чувствительность к шуму. Отметим достоинства применения OFDM.

1. За счет разбиения потока данных на множество потоков появляется возможность снижения скорости передачи в каждом из них, что позволяет использовать низкоскоростные модуляторы. Это упрощает их схему, уменьшает вычислительные затраты и вероятность ошибок демодуляции при наличии шумов и помех в принимаемом сигнале.

2. Вследствие прохождения сигнала через препятствия и отражения от них происходит искажение его частотного спектра: некоторые частотные составляющие сигнала (поднесущие) могут значительно ослабнуть при передаче и полезная информация на них будет потеряна, но на оставшихся поднесущих она может быть успешно восстановлена. Таким образом, при искажении спектра сигнала OFDM теряется только часть информации в отличие от обычного частотного или временного разделения сигналов.

3. Достаточно простые методы борьбы с межсимвольной интерференцией за счет введения защитного интервала.

4. Модуляция OFDM может быть выполнена в дискретной форме с использованием дискретного (ДПФ), а следовательно, и быстрого (БПФ) пре-

образования Фурье. Применение ДПФ (и особенно БПФ) ускоряет формирование и обработку сигнала, а также позволяет реализовать эти действия на любом сигнальном процессоре.

5.3. Спецификация IEEE 802.11a

Спецификация IEEE 802.11a стала исторически первой спецификацией, использующей диапазон частот 5 ГГц, что позволило немного разгрузить диапазон 2,4 ГГц, поскольку в нем не так много источников помех и значительно ниже средний уровень совокупных шумов. Однако в связи с дороговизной компонентов для оборудования 802.11a оно изначально не получило столь широкого распространения, как оборудование 802.11b, хотя их спецификации вышли практически одновременно.

Для оборудования 802.11a в России выделены две частотные полосы: 5150–5350 МГц и 5650–6425 МГц.

В спецификации 802.11a в качестве основного метода модуляции используется мультиплексирование с ортогональным частотным разделением (OFDM). Доступные для использования частотные диапазоны разбиваются на каналы шириной 20 МГц. При этом в каждом из каналов имеются 52 поднесущие частоты. Из них 48 используются для передачи данных, а остальные четыре — служебные. Расстояние между поднесущими составляет 0,3125 МГц. Ширина сигнальной полосы 16,66 МГц. Спектральная маска 802.11a показана на рис. 5.12.

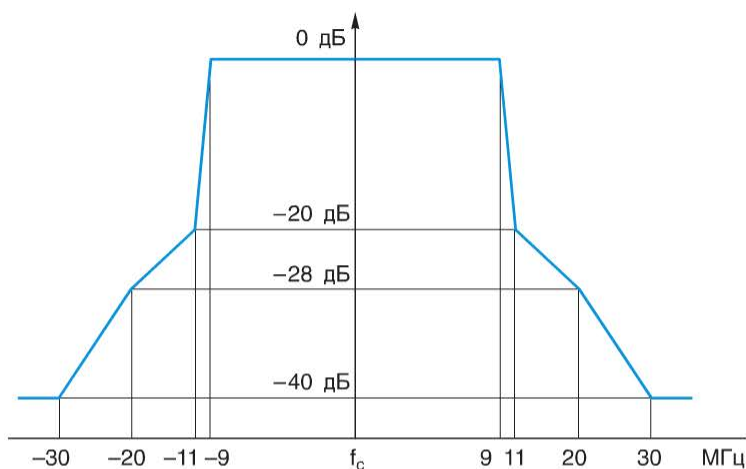


Рис. 5.12. Спектральная маска сигнала спецификации 802.11a

Спецификация 802.11a определяет следующие скорости передачи данных: 6, 9, 12, 18, 24, 36, 48 и 54 Мбит/с (табл. 5.4). Поддержка передачи и приема на скоростях 6, 12 и 24 Мбит/с является обязательной. Также допускается реализация и более высоких скоростей (до 108 Мбит/с).

В зависимости от требуемой скорости передачи поднесущие модулируются с использованием двухуровневой фазовой манипуляции (BPSK), квадратурной фазовой манипуляции (QPSK), 16- или 64-уровневой квадратурной амплитудной модуляции (16-QAM или 64-QAM).

Для прямой коррекции ошибок используется сверточный код со скоростью кодирования $1/2$, $2/3$ или $3/4$. Длительность защитного интервала 800 нс.

Таблица 5.4. Типы модуляции и скорости передачи данных 802.11a

Скорость передачи данных, Мбит/с	Модуляция	Скорость кодирования	Число кодированных битов на поднесущую	Число битов кода на символ OFDM	Число битов данных на символ OFDM
6	BPSK	$1/2$	1	48	24
9	BPSK	$3/4$	1	48	36
12	QPSK	$1/2$	2	96	48
18	QPSK	$3/4$	2	96	72
24	16-QAM	$1/2$	4	192	96
36	16-QAM	$3/4$	4	192	144
48	64-QAM	$2/3$	6	288	192
54	64-QAM	$3/4$	6	288	216

Необходимо обратить внимание, что диапазон 5 ГГц примыкает к частотам, которые частично используются наземными станциями слежения за спутниками связи. Для того чтобы нелегализуемое Wi-Fi-оборудование не мешало работе ведомственных систем, Европейским институтом по стандартизации в области телекоммуникаций (European Telecommunications Standards Institute, ETSI) были разработаны два дополнительных протокола: DFS (Dynamic Frequency Selection) и TPC (Transmit Power Control). С их помощью беспроводные устройства Wi-Fi могут автоматически менять частотные каналы или снижать излучаемую мощность в случаях возникновения коллизий на несущих частотах.

5.4. Спецификация IEEE 802.11b

Спецификация IEEE 802.11b стала первым широко используемым стандартом беспроводных устройств, и именно с ее выходом связано появление термина «Wi-Fi». Ограничение скорости в оригинальном стандарте 802.11 привело к тому, что устройства и беспроводные локальные сети этого типа практически не использовались. В 1999 году появилось высокоскоростное расширение спецификации 802.11 DSSS: *High Rate DSSS* (HR/DSSS PHY). Дополнительно к скоростям 1 и 2 Мбит/с это расширение предусматривало

передачу данных в диапазоне 2,4 ГГц на скоростях 5,5 и 11 Мбит/с. Ширина канала в 802.11b осталась прежней — 22 МГц. Формула для расчета центральной частоты канала приведена в табл. 5.5.

Таблица 5.5. Основные параметры IEEE 802.11b

Параметр	Значение
Диапазон частот	2400–2483,5 МГц
Метод расширения спектра	DSSS
План частот	$2412 + 5(n - 1), n = 1...13$
Скорости передачи данных и виды модуляции	1 Мбит/с — DBPSK 2 Мбит/с — DQPSK 5,5, 11 Мбит/с — CCK 22 Мбит/с — PBCC

В спецификации 802.11b для поддержки разных скоростей передачи используются разные схемы расширения спектра. Для работы на скоростях 1 и 2 Мбит/с — технология расширения спектра методом прямой последовательности (DSSS) с применением кодов Баркера, а для скоростей 5,5 и 11 Мбит/с — *комплементарные коды (Complementary Code Keying, CCK)*. В отличие от DSSS, где используются 11-разрядные коды, в CCK используются 8-разрядные коды, с помощью которых можно закодировать 4 или 8 бит информации в зависимости от требуемой скорости. При скорости передачи 11 Мбит/с кодируется 8 бит на символ, при скорости 5,5 Мбит/с в одном символе кодируется только 4 бит.

На рис. 5.13 показаны спектральная маска и спектр реального сигнала спецификации 802.11b. Как видно, форма сигнала имеет небольшие искажения вследствие влияния шумов и неидеальности частотных характеристик тракта прохождения сигнала. При этом мощность сигнала не превышает значений маски, что говорит о корректной работе беспроводного оборудования.

Важным достоинством спецификации 802.11b стало внедрение эффективного режима работы в условиях сильных помех и слабого сигнала. С этой целью используется динамический сдвиг скорости, позволяющий автоматически изменять скорость передачи данных в зависимости от уровня сигнала и помех. Так, например, в случае повышения уровня помех скорость передачи данных автоматически снижается до 5,5 или 2 или 1 Мбит/с. При уменьшении помех устройство возвращается к нормальному режиму работы на больших скоростях.

В расширенном варианте спецификации 802.11b+ определен опциональный метод кодирования — *Packet Binary Convolutional Coding (PBCC)*, который позволял достичь скорости передачи данных до 22 Мбит/с. Этот метод не получил широкого распространения и в настоящее время считается устаревшим.

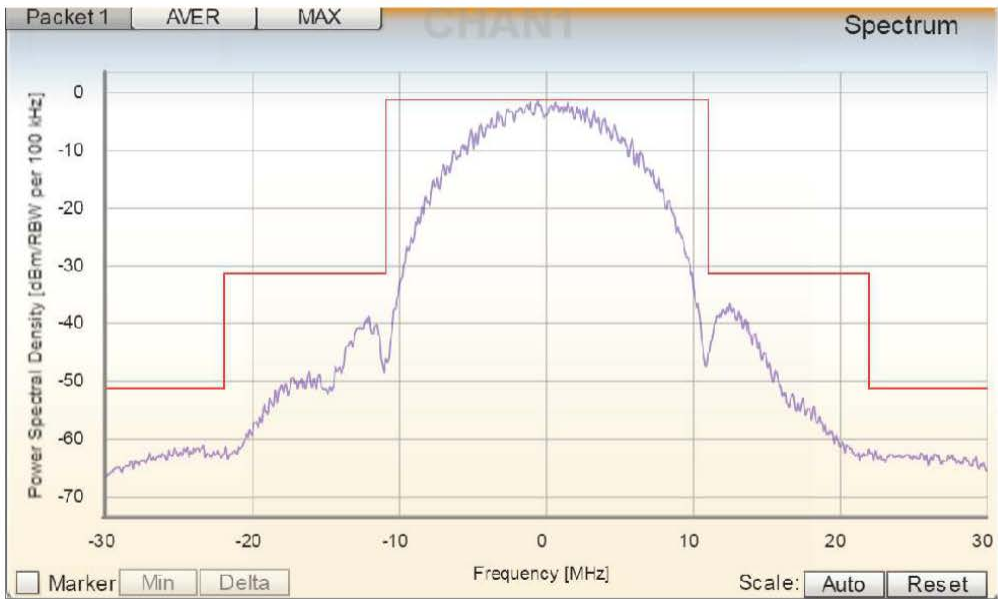


Рис. 5.13. Спектральная маска и спектр реального сигнала спецификации 802.11b

Внимание: максимальная скорость передачи данных, определяемая любой спецификацией 802.11, является максимально возможной теоретической пропускной способностью сети, достигаемой при использовании данной технологии. Однако реальная пропускная способность всегда меньше теоретической, что связано с издержками на передачу служебной информации, количеством клиентов, расстоянием, наличием преград, интерференцией и многим другим. Поддержание надежной работы и безопасности беспроводной сети снижает теоретическую скорость передачи данных примерно на 30...50 %.

5.5. Спецификация IEEE 802.11g

Следующим шагом на пути развития устройств Wi-Fi стала спецификация IEEE 802.11g, принятая в 2003 году. Она определяет физический уровень *Extended Rate PHY* (ERP) и, по сути, является высокоскоростным расширением спецификации 802.11b, которое позволяет передавать данные на скоростях до 54 Мбит/с в диапазоне 2,4 ГГц. Этот стандарт задумывался как универсальный, объединяющий в себе методы модуляции, использующиеся в двух предшествующих спецификациях: DSSS, CCK, OFDM и опционально PBCC. Таким образом, в 802.11g поддерживаются скорости передачи 1, 2, 5,5 и 11 Мбит/с (режим ERP-DSSS/CCK — аналогично 802.11b), 6, 12, 24, 36, 48 и 54 Мбит/с (режим ERP-OFDM — аналогично 802.11a). Поддержка передачи и приема данных

на скоростях 1, 2, 5,5, 6, 11, 12 и 24 Мбит/с является обязательной. При работе в опциональном режиме ERP-PBCC также определены две дополнительные скорости 22 и 33 Мбит/с. Существует еще один опциональный режим DSSS-OFDM, являющийся комбинацией модуляций DSSS и OFDM. Он определяет скорости передачи, аналогичные режиму ERP-OFDM. Два опциональных режима являются устаревшими и не рекомендуемыми к использованию. Следует отметить, что спецификация допускает также реализацию и более высоких скоростей (до 108 Мбит/с).

Для использования оборудования 802.11g в России выделена полоса частот 2400–2483,5 МГц. Ширина канала при работе в режиме ERP-DSSS/ССК составляет 22 МГц, при работе в режиме ERP-OFDM — 20 МГц. Спектральная маска при работе в режиме ERP-DSSS/ССК соответствует спектральной маске 802.11b. Спектральная маска при работе в режиме ERP-OFDM соответствует спектральной маске 802.11a. Формула для расчета плана частот приведена в табл. 5.6.

Таблица 5.6. Основные параметры IEEE 802.11g

Параметр	Значение
Диапазон частот	2400–2483,5 МГц
Режимы работы	DSSS/ССК, OFDM, PBCC, DSSS-OFDM
План частот	$2412 + 5(n - 1)$, $n = 1...13$
Скорости передачи данных и виды модуляции	1 Мбит/с — DBPSK 2 Мбит/с — DQPSK 5,5, 11 Мбит/с — ССК 6, 9 Мбит/с — BPSK 12, 18 Мбит/с — QPSK 24, 36 Мбит/с — 16-QAM 48, 54, 108 Мбит/с — 64-QAM 22, 33 Мбит/с — PBCC

Оборудование спецификации 802.11g полностью совместимо с оборудованием 802.11b. При одновременной работе в сети оборудования спецификаций 802.11g и 802.11b передача данных будет вестись на максимальной для оборудования 802.11b скорости.

5.6. Спецификация IEEE 802.11n

В сентябре 2009 года IEEE ратифицировал новое дополнение к стандарту 802.11, получившее название 802.11n. Оборудование спецификации 802.11n может работать в частотных диапазонах 2,4 и/или 5 ГГц со скоростью до 600 Мбит/с, что достигается благодаря использованию множества технологий, включая антенную технологию MIMO (*Multiple Input Multiple Output*), удвоение

ширины канала с 20 до 40 МГц и агрегацию кадров на MAC-подуровне. При этом сохраняется совместимость со спецификацией 802.11a в диапазоне 5 ГГц и спецификациями 802.11b/g в диапазоне 2,4 ГГц.

5.6.1. Технологии повышения производительности на физическом уровне 802.11n

Спецификация 802.11n определяет новый физический уровень с высокой производительностью (*High Throughput, HT*) для систем OFDM (HT PHY) (рис. 5.14). Он основан на физическом уровне OFDM и включает следующие обязательные функции, расширяющие возможности OFDM с целью повышения производительности сети:

- использование технологии МИМО и до четырех пространственных потоков;
- использование каналов шириной 40 МГц;
- увеличение количества поднесущих OFDM.

Также определено несколько опциональных функций, служащих для повышения скорости передачи и увеличения дальности действия беспроводной сети:

- формирование *диаграммы направленности передатчика (transmit beam-forming, TxBF)*;
- использование *пространственно-временного блочного кодирования (space-time block coding, STBC)*;
- использование укороченного защитного интервала (*Short GI*).

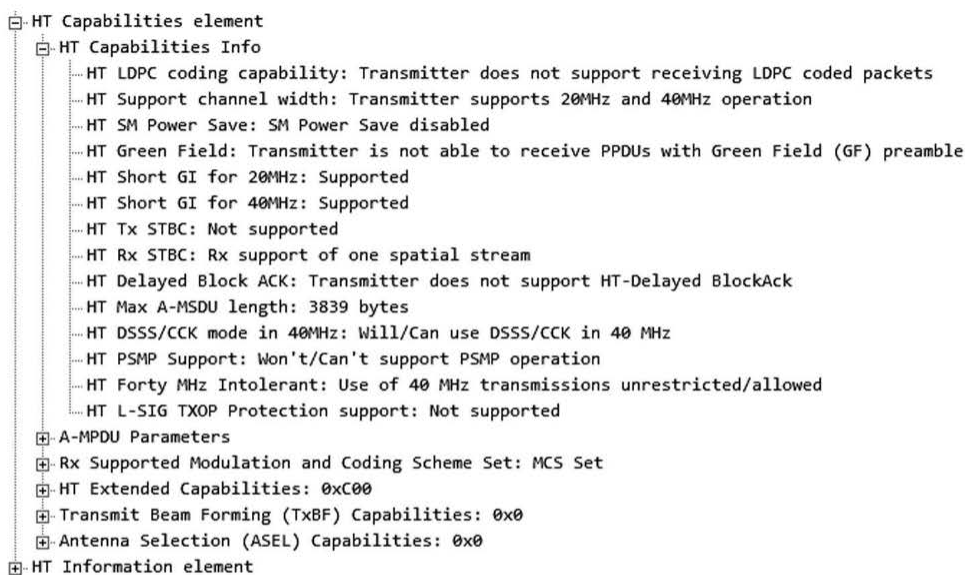


Рис. 5.14. Возможности физического уровня HT, указанные в кадре Beacon

Понятие MIMO

В технологиях беспроводных сетей MIMO является радиоантенной технологией, использующей множество антенн и преимущества многолучевого распространения сигналов для передачи и приема данных.

Существует несколько форм MIMO (рис. 5.15):

- *Single Input Single Output (SISO)*: простейшая форма MIMO, в которой передатчик и приемник имеют одну антенну. Эта конфигурация являлась традиционной формой организации беспроводного канала в сетях 802.11 до появления спецификации 802.11n.

- *Single Input Multiple Output (SIMO)*: форма MIMO, в которой передатчик имеет только одну антенну, а приемник множество.

- *Multiple Input Single Output (MISO)*: форма MIMO, в которой передатчик имеет множество антенн, приемник только одну.

- *Multiple Input Multiple Output (MIMO)*: форма MIMO, в которой передатчик и приемник имеют множество антенн. Эта конфигурация MIMO используется в спецификации 802.11n.

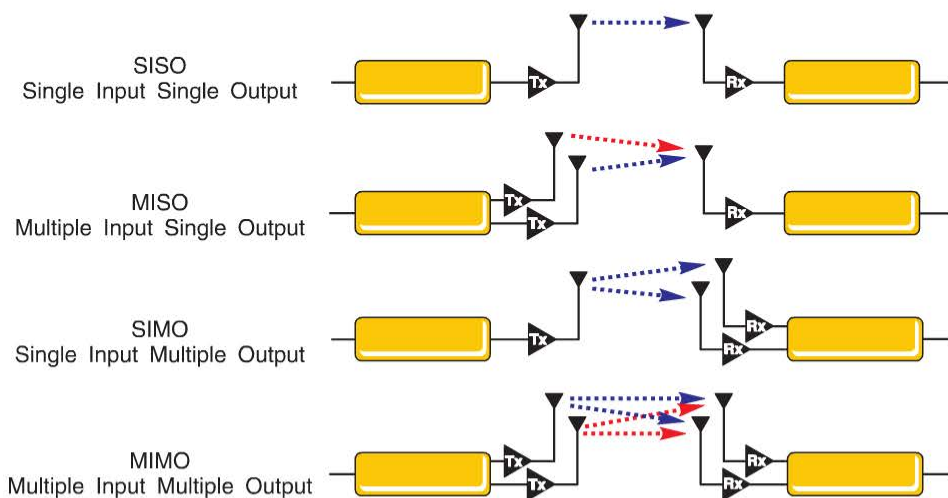


Рис. 5.15. Формы MIMO

Перечисленные формы MIMO являются *многоантенными (Multi-antenna)* или *однопользовательскими (Single-User MIMO, SU-MIMO)*. Однопользовательские формы MIMO позволяют одновременно передавать потоки данных только одному устройству. Существуют также *многопользовательские* формы MIMO (*Multi-User MIMO, MU-MIMO*). В данном разделе речь пойдет только об однопользовательской форме MIMO, поскольку именно она реализована на физическом уровне 802.11n.

Системы MIMO могут использовать различные технологии для повышения скорости и увеличения дальности действия сети:

- пространственное мультиплексирование;
- формирование диаграммы направленности передатчика;
- пространственное кодирование.

В основе технологии MIMO лежит *пространственное мультиплексирование* (*spatial multiplexing*), при использовании которого независимые потоки данных передаются через множество антенн.

Внимание: спецификации 802.11a/b/g использовали простейшую антенную технологию SISO: прием и передача выполняются с помощью одной антенны через один канал.

Несмотря на то что многие устройства 802.11a/b/g имеют две антенны, они не могут в отличие от устройств с поддержкой MIMO одновременно использовать их для передачи сигналов. Также антенны не могут использоваться для одновременного приема сигналов. Каждая антенна получает копию сигнала разной мощности, и устройство выбирает наиболее мощный из них для дальнейшей обработки, в результате чего в процессе приема информации используется только одна антенна, обеспечивающая наилучший прием. Этот метод называется пространственным разнесением антенн и позволяет бороться с интерференцией сигналов. Для отправки сигнала устройство обычно выбирает антенну, которая использовалась для получения последнего сигнала.

В системах MIMO передаваемый поток данных разбивается на независимые последовательности битов (*пространственные потоки*, *spatial stream*), которые пересылаются одновременно с использованием разных антенн. Это позволяет единовременно передать большой объем данных по сравнению с использованием одной антенны. При этом антенны передают данные независимо друг от друга и в одном и том же частотном диапазоне, но по разным направлениям в пространстве. Другими словами, в технологии MIMO реализовано несколько пространственно разнесенных подканалов, по которым данные передаются одновременно в одном и том же частотном диапазоне. В простейшем случае это выглядит как передатчик с двумя антеннами и приемник с двумя антеннами, в которых по каждому каналу одновременно и независимо передаются и принимаются потоки данных (рис. 5.16).

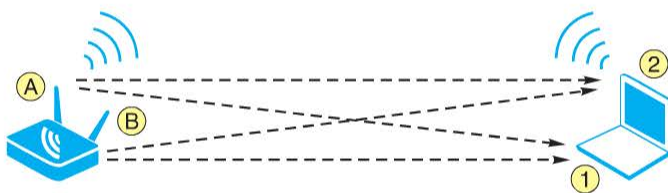


Рис. 5.16. Передача с двумя пространственными потоками MIMO

В случае прямой видимости все приемные антенны получают одинаковые сигналы от передатчиков. Однако если на пути следования переданных сигналов встречаются препятствия, в результате многолучевого распространения

приемные антенны могут получить разные сигналы (рис. 5.17). Для систем SISO многолучевое распространение приводит к межсимвольной интерференции и уменьшению производительности сети, а системы MIMO используют его для достижения высоких скоростей передачи.

Следует также отметить преимущества спецификации 802.11n при реализации SIMO и MISO. В отличие от предыдущих спецификаций, в которых при наличии нескольких приемных антенн (при реализации SIMO) прием осуществляется только одной антенной, выдающей максимальный сигнал, в новой спецификации на приемнике имеется возможность анализа всех копий сигнала и их комбинации с помощью технологии MRC (*Maximum Ratio Combined*). Алгоритм работы MRC подразумевает сбор всех прямых и отраженных при многолучевом распространении сигналов на нескольких антеннах и приемниках. Далее процессор (DSP) отбирает лучший сигнал с каждого приемника и выполняет их комбинирование. Математическая обработка сигналов реализует виртуальный фазовый сдвиг для создания положительной интерференции со сложением сигналов. Это приводит к тому, что характеристики результирующего суммарного сигнала превосходят характеристики всех исходных сигналов. MRC позволяет значительно улучшить условия работы маломощных мобильных устройств в сети Wi-Fi.

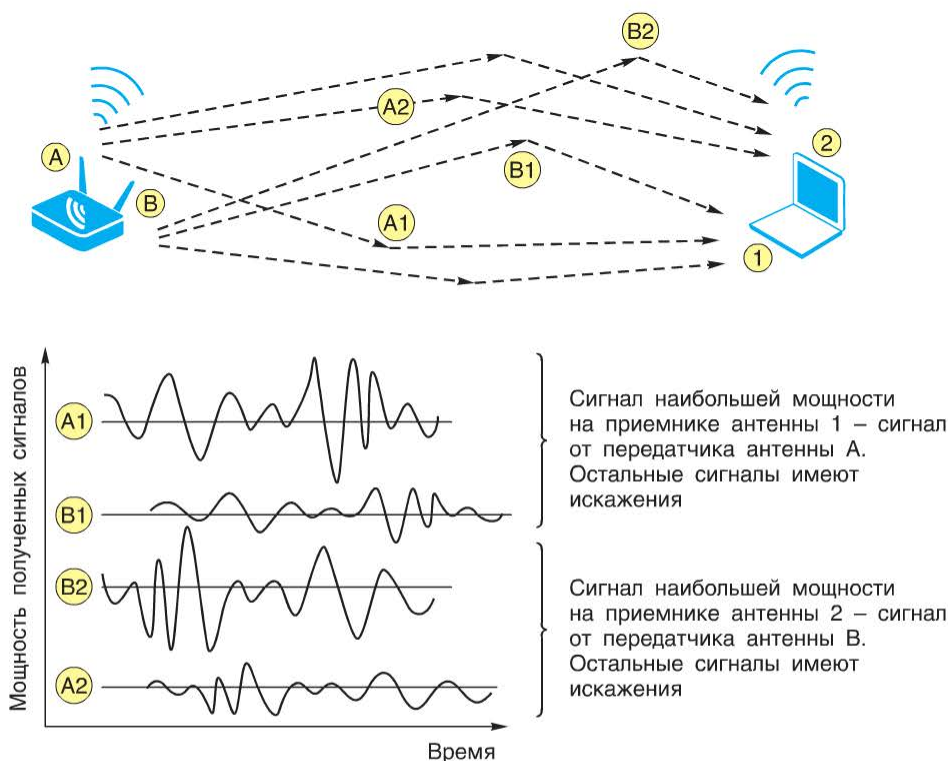


Рис. 5.17. Прием сигналов в системах MIMO

При реализации MISO, если, например, передающая станция имеет не менее двух связанных передатчиков с разнесенными антеннами, а принимающий клиент имеет только одну антенну, возникает возможность отправки группы идентичных сигналов для увеличения количества копий передаваемой информации. Это позволяет повысить надежность передачи информации и снизить необходимость повторной передачи данных в радиоканале в случае их потерь.

Следует отметить, что в зависимости от аппаратной реализации устройств количество антенн не всегда совпадает с количеством передаваемых пространственных потоков: антенн может быть больше, чем потоков, что обеспечивает более качественный прием данных. Всего в спецификации 802.11n определено использование до четырех пространственных потоков, при этом большинство наборов микросхем 802.11n поддерживает работу только с двумя или тремя пространственными потоками.

Поскольку оборудование 802.11n использует множество антенн и множество пространственных потоков для передачи данных, конфигурация MIMO описывается набором цифр, указывающих количество антенн для передачи данных (T), количество антенн для приема данных (R), количество пространственных потоков данных (S) (рис. 5.18).



Рис. 5.18. Обозначение конфигурации MIMO оборудования 802.11n

Например, запись 2x2:2 говорит о том, что в устройстве 802.11n используется конфигурация MIMO с двумя передающими, двумя приемными антеннами и два пространственных потока данных. Спецификация 802.11n определяет конфигурации MIMO от 2x1:1 до 4x4:4.

Формирование диаграммы направленности передатчика

Одним из сложных вопросов в системах MIMO является организация эффективного приема сигналов, отправленных с разных антенн. Существует несколько способов повышения эффективности MIMO. Один из них, используемый в спецификации 802.11n, — технология *формирования диаграммы направленности передатчика* (*transmit beamforming, TxBF*), также называется *технологией формирования направленного луча*. Этот метод является хорошо известным и широко применяемым в радиотехнике. При его использовании в беспроводных сетях он помогает точке доступа, оборудованной всенаправленной антенной, фокусировать энергию в сторону определенного клиента, а клиентскому устройству — в сторону точки доступа, что позволяет повысить

отношение сигнал/шум и соответственно расстояние передачи (рис. 5.19). Передатчик, который фокусирует энергию в сторону приемника, называется *формирователем луча (beamformer)*, а устройство, которое получает сфокусированную энергию, — *получателем луча (beamformee)*. Любая беспроводная станция может быть как формирователем, так и получателем луча.



Рис. 5.19. Технология формирования диаграммы направленности передатчика

Целью метода формирования диаграммы направленности передатчика является когерентный прием сигналов. Для этого с множества антенн передатчика передаются одинаковые сигналы, но с незначительным сдвигом по времени (фазе). На стороне приемника полученные сигналы складываются, формируя единый сигнал. Такой подход приводит к наименьшему искажению передаваемых сигналов, позволяет значительно увеличить дальность действия беспроводной сети и уменьшает вероятность нарушения связи.

Технология формирования диаграммы направленности передатчика использует массив антенн для динамического изменения схемы излучения точки доступа. Эта схема может изменяться на кадровом уровне. Поскольку широкоэмиттерный или многоадресный трафик получают множество станций, то точка доступа с поддержкой функции формирования диаграммы направленности для передачи такого трафика будет использовать всенаправленную диаграмму направленности.

Передача пространственных потоков в системах с множеством антенн включает сложные векторные и матричные алгоритмы обработки: необходи-

мо постоянно запрашивать информацию по идентификации канала, его состоянию и конкретным параметрам (*Channel State Information, CSI*). Функция формирования диаграммы направленности передатчика оценивает состояние канала и определяет, как наилучшим образом использовать доступную мощность излучения для передачи сигнала клиенту. Для описания того, как направлять излучаемую энергию в сторону получателя, используется *управляющая матрица (steering matrix)*, которая определяет настройку каждого антенного элемента передатчика.

Спецификация 802.11n определяет два метода оценки канала: *implicit feedback (неточная оценка)* и *explicit feedback (точная оценка)*. Результатом любого из методов оценки канала является вычисление управляющей матрицы. Определение состояния канала выполняется в процессе обмена «изучающими» кадрами (*sounding frame*) между формирователем и получателем луча. Этот процесс использует некоторую разновидность обратной связи между ними. В методе неточной оценки получатель луча отправляет формирователю длинные обучающие символы, с помощью которых формирователь оценивает состояние канала между ними и вычисляет управляющую матрицу для передачи данных. В методе точной оценки формирователь луча выполняет непосредственную оценку состояния канала путем отправки длинных обучающих символов получателю. Получатель может ответить информацией о состоянии канала связи или сжатой управляющей матрицей на основе изучения полученных обучающих символов (рис. 5.20).

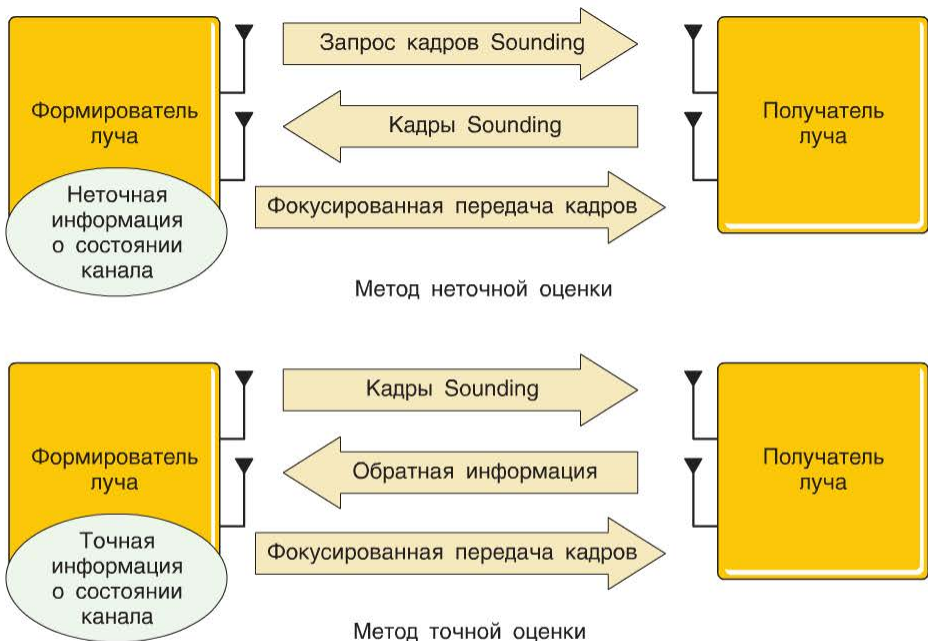


Рис. 5.20. Методы оценки канала

Функция формирования диаграммы направленности является необязательной, поэтому производители не всегда реализуют ее поддержку в устройствах. Для того чтобы воспользоваться ее преимуществами в сети, она должна поддерживаться как точкой доступа, так и клиентским устройством, при этом точка доступа и клиент должны поддерживать одинаковую реализацию функции (одинаковые методы оценки канала). Устройство, поддерживающее функцию формирования диаграммы направленности, должно сообщать об этой возможности в кадрах Beacon или Association Request. Если одно из взаимодействующих устройств не поддерживает эту функции или варианты реализации функции разные, оба устройства будут работать в обычном режиме.

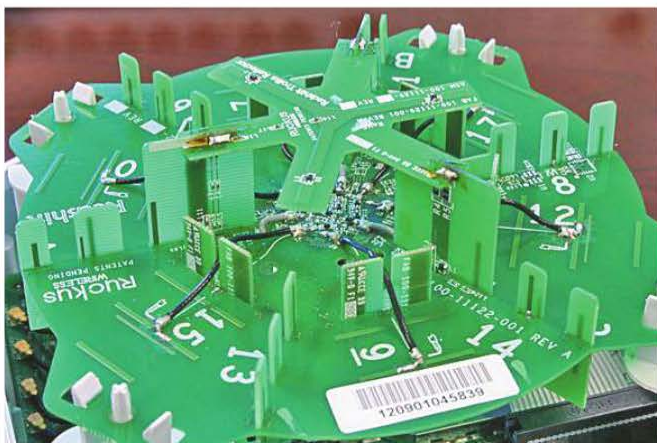


Рис. 5.21. Антенная система точки доступа Ruckus 7962

Следует отметить, что формирование направленной передачи можно осуществлять за счет переключения антенн из набора направленных антенн (рис. 5.21): на некоторых точках доступа может устанавливаться набор направленных антенн, позволяющий формировать диаграмму направленности в сторону клиента простым переключением между ними, что существенно упрощает управление лучом.

Пространственно-временное блочное кодирование

Еще одним методом повышения надежности и скорости передачи в беспроводной сети является *пространственно-временное блочное кодирование* (*space-time block coding, STBC*). Оно применяется в том случае, когда количество передающих антенн больше количества пространственных потоков. Например, точка доступа имеет три антенны, а клиентское устройство — две. STBC использует кодирование для передачи нескольких копий одного потока данных через разные антенны и на разных скоростях в зависимости от состояния подканалов. Это позволяет значительно повысить надежность

передачи и снизить количество ошибок, так как передатчик сможет наилучшим образом восстановить исходные данные, расшифровав и сравнив принятые пространственные потоки (рис. 5.22).

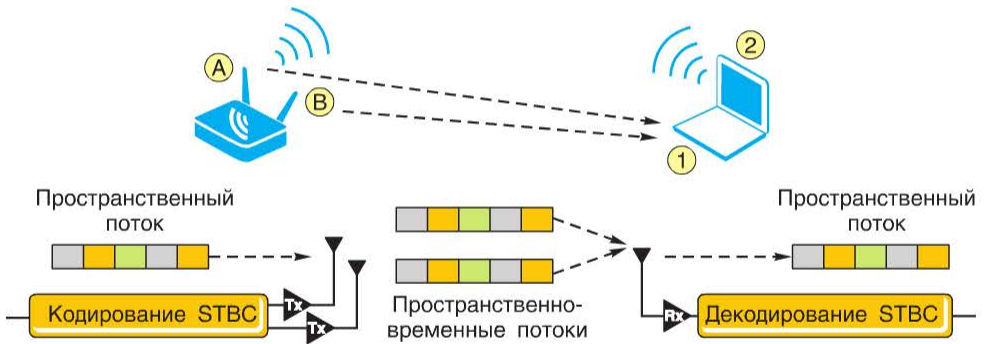


Рис. 5.22. Пространственно-временное кодирование

Рассмотрим пространственно-временное кодирование подробнее. Принцип кодирования состоит в том, что передаваемая последовательность битов разбивается на две пары А и В (например, на четные и нечетные символы). Для передачи такого блока требуется два излучателя и два временных интервала передачи. В первом временном интервале антенна 1 будет излучать символ А, а антенна 2 — символ В. Во втором временном интервале антенна 1 передает В*, а антенна 2 — А*. Поскольку передаваемая информация разделяется в пространстве и времени, то передаваемые потоки данных называются пространственно-временными. Зависимость числа пространственных потоков от числа передающих и приемных антенн с применением STBC и без него показана в табл. 5.7, взятой из стандарта IEEE 802.11-2012.

Таблица 5.7. Число пространственно-временных потоков

Число передающих антенн	Число приемных антенн	Число пространственно-временных потоков без STBC	Число пространственно-временных потоков с STBC
1	1	1	—
2	1	1	2
3	1	1	2
3	2	2	3
4	1	1	2
4	2	2	4

Каналы шириной 40 МГц

В предыдущих спецификациях 802.11 для передачи сигналов в диапазонах 2,4 и 5 ГГц использовались каналы шириной около 20 МГц. Спецификация 802.11n определяет использование каналов шириной 20 МГц в диапазонах 2,4 и 5 ГГц и добавляет режим, в котором используются рабочие каналы шириной 40 МГц.

Для получения канала шириной 40 МГц два соседних канала вместе с защитными интервалами между ними можно объединить (рис. 5.23–5.26). Увеличение ширины канала в 2 раза приводит к двукратному увеличению скорости передачи.

Для оборудования спецификации 802.11n в России выделены одна полоса в диапазоне 2,4 ГГц (2400–2483,5 МГц) и две полосы в диапазоне 5 ГГц: (5150–5350 МГц и 5650–6425 МГц).

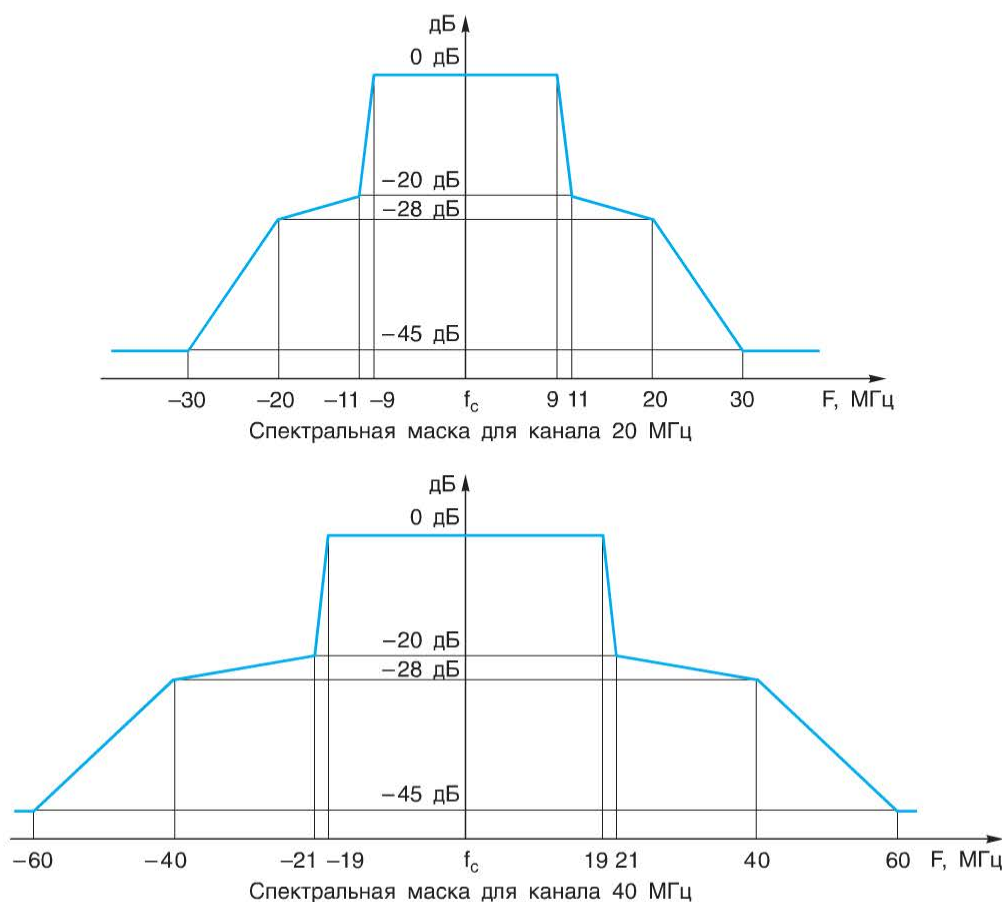


Рис. 5.23. Спектральные маски сигналов спецификации 802.11n для каналов 20 и 40 МГц в диапазоне 2,4 ГГц

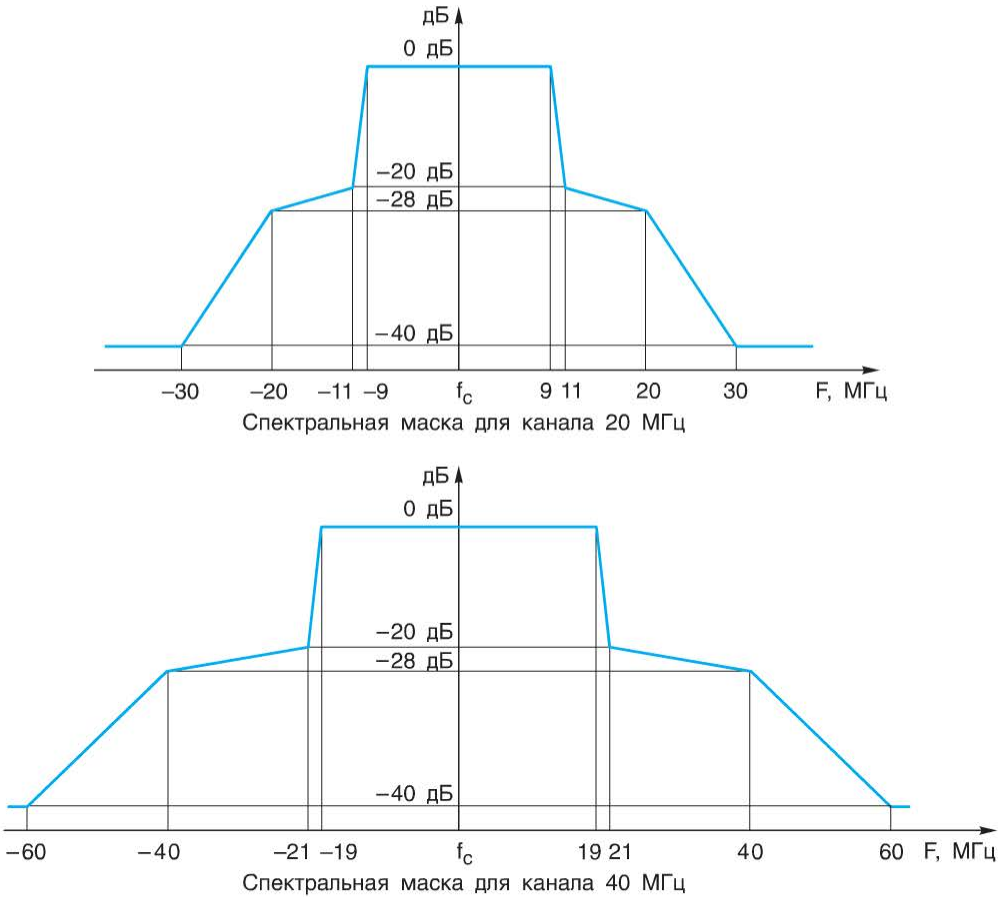


Рис. 5.24. Спектральные маски сигналов спецификации 802.11p для каналов 20 и 40 МГц в диапазоне 5 ГГц

В диапазоне 5 ГГц доступно множество каналов шириной 40 МГц. Ограниченная ширина диапазона 2,4 ГГц делает использование каналов шириной 40 МГц неудобным. В отличие от диапазона 5 ГГц, в котором между центральными частотами соседних каналов расстояние 20 МГц, в диапазоне 2,4 ГГц расстояние между центральными частотами каналов 5 МГц. Если учесть ограниченную ширину спектра в диапазоне 2,4 ГГц (83,5 МГц), то для использования доступно только три неперекрывающихся канала (1, 6 и 11) шириной 20 МГц. При использовании каналов шириной 40 МГц (рис. 5.27) возникают следующие проблемы:

- из-за ограниченного спектра в диапазоне 2,4 ГГц может быть только два непересекающихся канала — один канал шириной 40 МГц и один канал шириной 20 МГц;
- невозможно построить канал шириной 40 МГц, используя два соседних канала шириной 20 МГц.

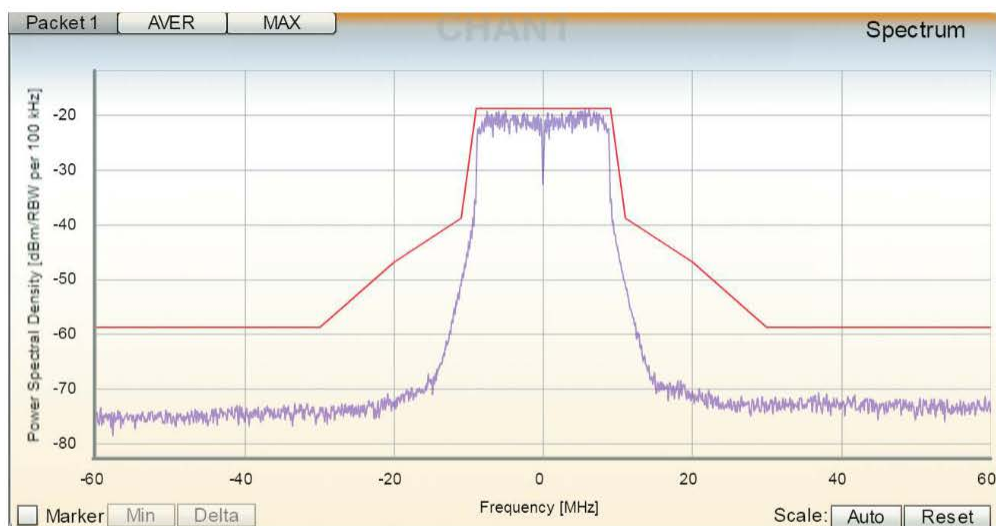


Рис. 5.25. Спектральная маска спецификации 802.11n для канала 20 МГц и спектр реального сигнала в диапазоне 2,4 ГГц

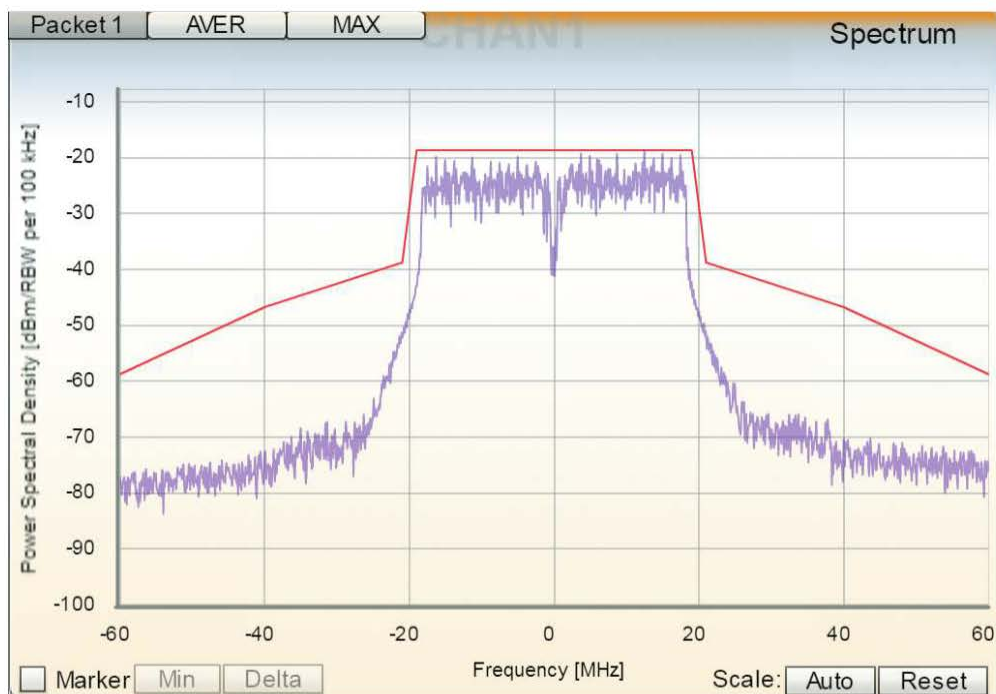


Рис. 5.26. Спектральная маска спецификации 802.11n для канала 40 МГц и спектр реального сигнала в диапазоне 2,4 ГГц

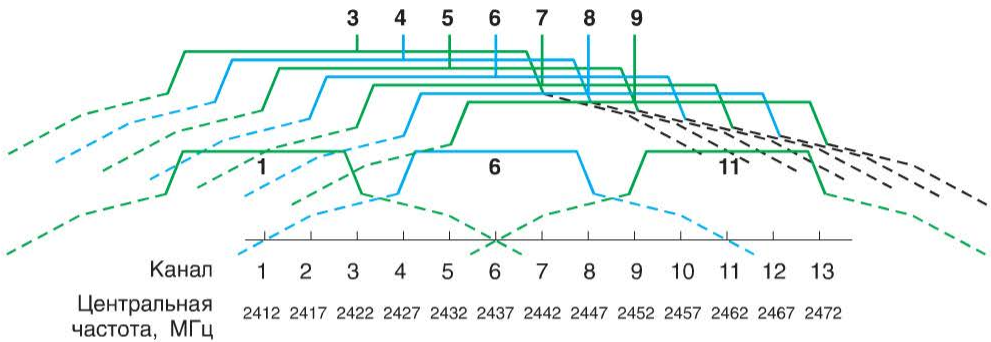


Рис. 5.27. Каналы 40 МГц спецификации 802.11n, доступные в диапазоне 2,4 ГГц

В связи с этим не рекомендуется использовать каналы шириной 40 МГц в диапазоне 2,4 ГГц, так как это приводит к неэффективному использованию радиочастотного ресурса и повышает вероятность интерференции с оборудованием 802.11b/g.

Для создания корпоративных беспроводных сетей 802.11n в большинстве случаев используется диапазон 5 ГГц (рис. 5.28), так как его спектр шире, чем у 2,4 ГГц, и он менее загружен различными сигналами стороннего оборудования и помехами.

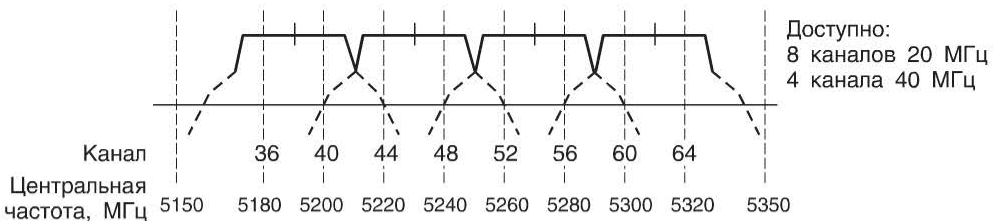


Рис. 5.28. Каналы 40 МГц спецификации 802.11n, доступные в полосе 5150–5350 МГц

Следует сказать о нумерации каналов 40 МГц. В основе частотного планирования каналов 802.11n лежат каналы шириной 20 МГц. Даже при использовании каналов шириной 40 МГц, они обозначаются как «основной» или «первичный» (*primary*) канал 20 МГц и «вторичный» (*secondary*) канал 20 МГц. Название канала 40 МГц состоит из двух полей: номера основного канала и направления смещения относительно него вторичного канала («1» обозначает выше, «-1» — ниже). Например, канал шириной 40 МГц в диапазоне 2,4 ГГц может быть сформирован из каналов 1 и 5 и обозначаться как 1+ (1,1) или 5- (5, -1) в зависимости от того, какой канал является основным. В диапазоне 5 ГГц канал шириной 40 МГц может использовать, например, каналы 36 и 40 и обозначаться как 36+ (36, 1) или 40- (40, -1). Настройка каналов 40 МГц на точке доступа D-Link DWL-3600AP показана на рис. 5.29.

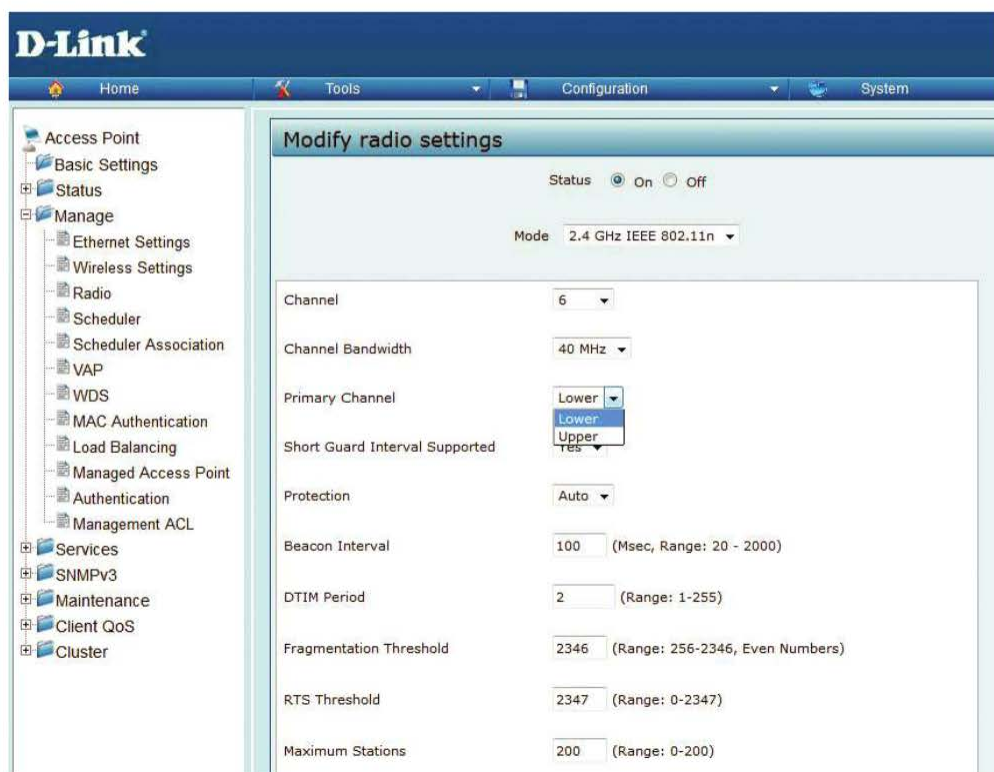


Рис. 5.29. Настройка канала 40 МГц на точке доступа D-Link DWL-3600AP

Увеличенное количество поднесущих

Физический уровень HT PHY основан на физическом уровне OFDM. По сравнению со спецификациями 802.11a/g количество поднесущих в канале шириной 20 МГц увеличилось с 52 до 56 (52 рабочих и 4 служебных). В канале шириной 40 МГц используется 114 поднесущих (108 рабочих и 6 служебных) (рис. 5.30). Благодаря увеличению количества поднесущих увеличивается количество подканалов, по которым могут передаваться данные, что в целом повышает скорость передачи.

Схемы прямого исправления ошибок в 802.11n

Для борьбы с ошибками в передаваемых кадрах 802.11n используются две схемы прямого исправления ошибок (FEC). Дополнительно к сверточным кодам, определенным на физическом уровне OFDM, добавлена опциональная поддержка кодов LDPC (*Low-Density Parity Check*). Сверточные коды, используемые в 802.11n, идентичны кодам, используемым в 802.11a/g. Для повышения эффективной скорости физического уровня к ранее определенным скоростям кодирования 1/2, 2/3, 3/4 добавлена новая скорость кодирования 5/6.

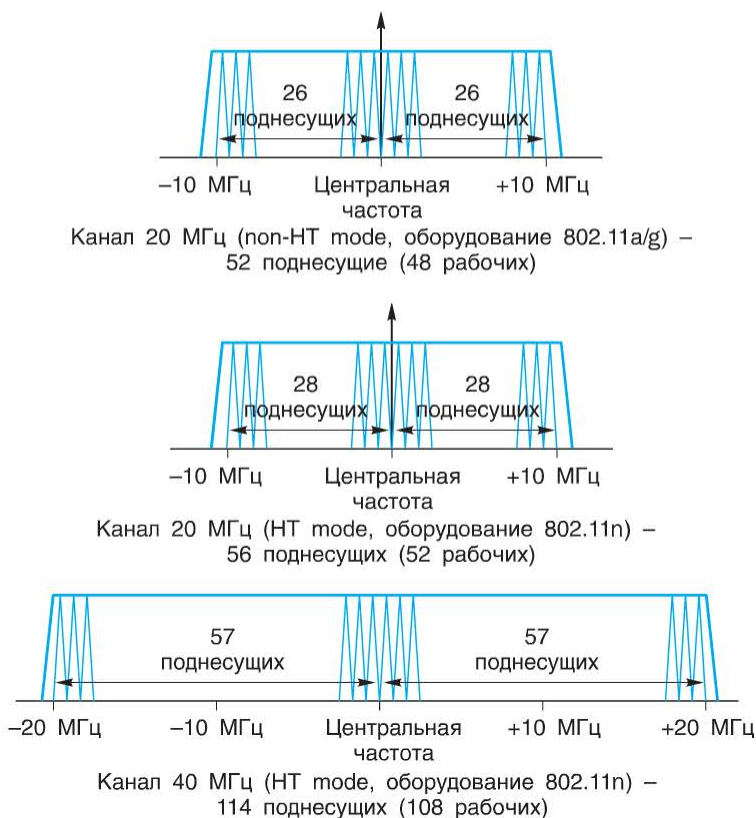


Рис. 5.30. Количество поднесущих OFDM 802.11a/g и 802.11n

Коды LDPC имеют большую производительность по сравнению со сверточными кодами, однако требуют более сложной схемотехники оборудования. Коды LDPC так же, как и сверточные коды, разбивают данные на блоки и к каждому блоку добавляют избыточные биты, позволяющие выявлять ошибки. Устройство, поддерживающее кодирование LDPC, должно сообщать об этой возможности в кадрах Beacon или Association Request. Использование кодов LDPC возможно только в случае их поддержки взаимодействующими устройствами.

Укороченный защитный интервал

Напомним, что защитный интервал используется в OFDM для борьбы с межсимвольной интерференцией и интерференцией между поднесущими. Защитный интервал представляет собой циклическое повторение окончания OFDM-символа. Он добавляется перед передаваемым OFDM-символом в передатчике и удаляется при приеме символа в приемнике. Наличие защитного интервала создает временные паузы между отдельными символами. В спецификациях 802.11a/g используется защитный интервал длительностью

800 нс. В спецификации 802.11n сохранился защитный интервал 800 нс и появился опциональный режим, позволяющий использовать укороченный защитный интервал (Short GI) длительностью 400 нс.

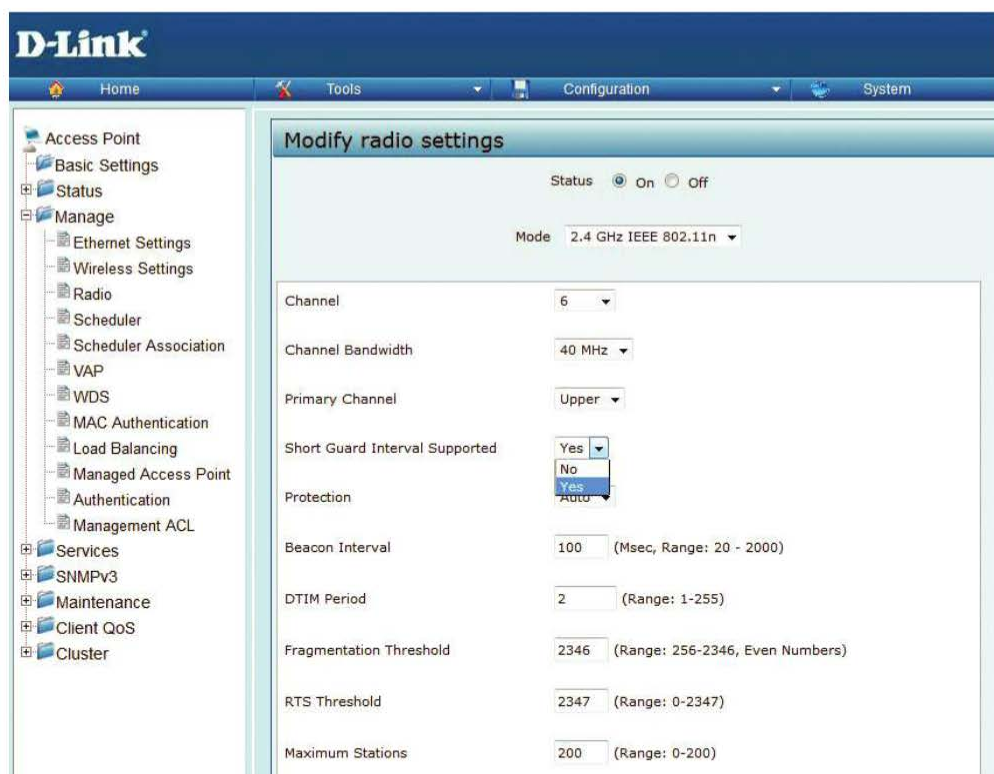


Рис. 5.31. Настройка укороченного защитного интервала на точке доступа D-Link DWL-3600AP

На беспроводных устройствах D-Link можно настроить использование укороченного защитного интервала (рис. 5.31). При этом скорость передачи в сети увеличивается примерно на 10 % при таких условиях окружающей среды, в которых задержки между кадрами минимальны. Например, укороченный защитный интервал можно использовать в большинстве случаев при создании беспроводных сетей внутри помещений. В уличных беспроводных сетях использовать укороченный защитный интервал не рекомендуется, так как это может привести к большому количеству ошибок.

Модуляция и схемы кодирования

Скорость передачи в 802.11n зависит от количества пространственных потоков, ширины канала, используемых схем модуляции и сверточного кодирования, длительности защитного интервала.

В связи с тем, что в 802.11n существует 77 возможных комбинаций этих параметров, для определения скорости передачи в спецификации была введена *схема модуляции и кодирования (Modulation and Coding Scheme, MCS)*. Номер схемы MCS (*MCS Index*) является целым числом, назначаемым каждой из комбинаций модуляции, скорости кодирования и количества пространственных потоков.

Модуляция сигнала заключается в изменении какого-либо параметра (амплитуды или фазы) опорного сигнала по закону модулирующей последовательности данных, подлежащей передаче. Применяется модуляция после кодирования, чередования и разбиения данных на n поднесущих и предшествует формированию OFDM-символа посредством ОБПФ. В качестве допустимых модуляций используются двухуровневая фазовая манипуляция (BPSK), квадратурная фазовая манипуляция (QPSK), квадратурная амплитудная модуляция (*Quadrature Amplitude Modulation, QAM*) с 16 и 64 уровнями. На рис. 5.32 показана модуляция BPSK.

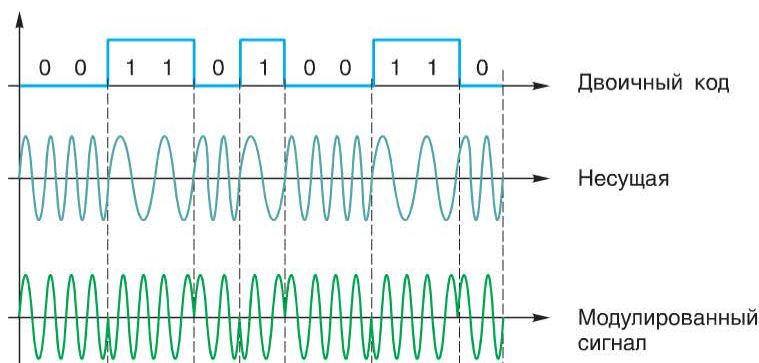


Рис. 5.32. Модуляция BPSK

Выбор вида модуляции зависит от требуемой скорости передачи данных и отношения сигнал/шум, поскольку чем сложнее модуляция, тем большее отношение сигнал/шум требуется для обеспечения правильной демодуляции. Модуляция выполняется блоком MAP (*mapping*) передатчика и может быть представлена *сигнальным созвездием (constellation)*, т. е. отображением на некоторой плоскости возможных комбинаций сигнала, как показано на рис. 5.33.

Количество точек на сигнальном созвездии соответствует числу информационных позиций, т. е. для BPSK имеем 2 точки и т. д. Дополнительные точки на сигнальном созвездии, появляющиеся на главных осях в точках $(0, 1)$, $(0, -1)$, $(-1, 0)$ и $(1, 0)$, образуются опорными пилотными сигналами (выделены красным на рис. 5.33).

Пространственные потоки данных могут использовать как одинаковые, так и разные типы модуляции и скорости кодирования. Использование одинаковых параметров передачи для всех потоков называется *равной модуляцией (Equal Modulation)*, а разных параметров — *неравной модуляцией (Unequal Modulation)*.

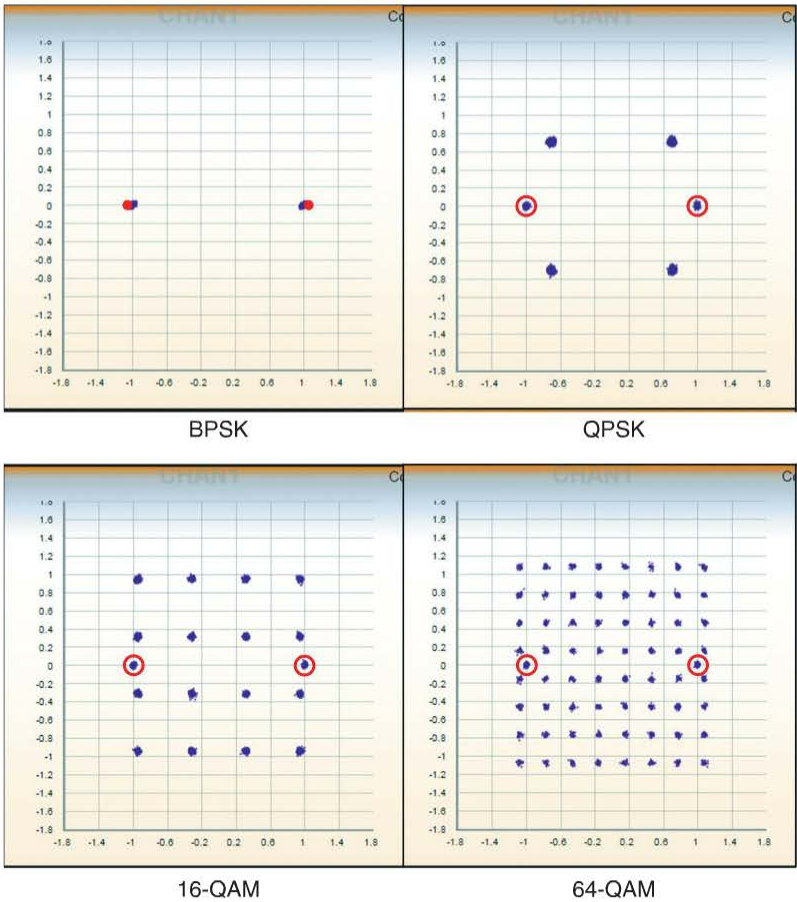


Рис. 5.33. Сигнальные созвездия BPSK, QPSK, 16-QAM и 64-QAM

Схемы MCS с номерами от 0 до 31 определяют использование одинаковой модуляции и кодирования во всех потоках. В оборудовании 802.11n применяются в основном схемы с равной модуляцией. Наиболее широко используемые схемы MCS приведены в табл. 5.8.

Схемы модуляции с номерами от 32 до 76 описывают смешанные комбинации на разных пространственных потоках. Например, MCS33 описывает использование модуляции 16-QAM на пространственном потоке 1 и QPSK на пространственном потоке 2; MCS76 — модуляции 64-QAM на пространственных потоках 1, 2, 3 и 16-QAM на пространственном потоке 4. Использование неравной модуляции полезно в том случае, если один из потоков подвергается большему воздействию негативных факторов по сравнению с другими.

Таблица 5.8. Схемы MCS

Номер схемы	Модуляция	Число простран- ственных потоков	Скорость передачи данных, Мбит/с (ширина канала 20 МГц)		Скорость передачи данных, Мбит/с (ширина канала 40 МГц)	
			Защитный интервал 800 нс	Защитный интервал 400 нс (опционально)	Защитный интервал 800 нс	Защитный интервал 400 нс (опционально)
0	BPSK	1	6,50	7,20	13,50	15,00
1	QPSK	1	13,00	14,40	27,00	30,00
2	QPSK	1	19,50	21,70	40,50	45,00
3	16-QAM	1	26,00	28,90	54,00	60,00
4	16-QAM	1	39,00	43,30	81,00	90,00
5	64-QAM	1	52,00	57,80	108,00	120,00
6	64-QAM	1	58,50	65,00	121,50	135,00
7	64-QAM	1	65,00	72,20	135,00	150,00
8	BPSK	2	13,00	14,40	27,00	30,00
9	QPSK	2	26,00	28,90	54,00	60,00
10	QPSK	2	39,00	43,30	81,00	90,00
11	16-QAM	2	52,00	57,80	108,00	120,00
12	16-QAM	2	78,00	86,70	162,00	180,00
13	64-QAM	2	104,00	115,60	216,00	240,00
14	64-QAM	2	117,00	130,00	243,00	270,00
15	64-QAM	2	130,00	144,40	270,00	300,00
16	BPSK	3	19,50	21,70	40,50	45,00
17	QPSK	3	39,00	43,30	81,00	90,00
18	QPSK	3	58,50	65,00	121,50	135,00
19	16-QAM	3	78,00	86,70	162,00	180,00
20	16-QAM	3	117,00	130,00	243,00	270,00
21	64-QAM	3	156,00	173,30	324,00	360,00
22	64-QAM	3	175,50	195,00	364,50	405,00
23	64-QAM	3	195,00	216,70	405,00	450,00
24	BPSK	4	26,00	28,90	54,00	60,00
25	QPSK	4	52,00	57,80	108,00	120,00
26	QPSK	4	78,00	86,70	162,00	180,00
27	16-QAM	4	104,00	115,60	216,00	240,00
28	16-QAM	4	156,00	173,30	324,00	360,00
29	64-QAM	4	208,00	231,10	432,00	480,00

Номер схемы	Модуляция	Число простран- ственных поток	Скорость передачи данных, Мбит/с (ширина канала 20 МГц)		Скорость передачи данных, Мбит/с (ширина канала 40 МГц)	
			Защитный интервал 800 нс	Защитный интервал 400 нс (опционально)	Защитный интервал 800 нс	Защитный интервал 400 нс (опционально)
30	64-QAM	4	234,00	260,00	486,00	540,00
31	64-QAM	4	260,00	288,90	540,00	600,00

При настройке некоторых беспроводных устройств администратор может самостоятельно выбрать используемые схемы модуляции и кодирования (рис. 5.34).

Transmit Power

100 (Percent, Range: 1 - 100)

Fixed Multicast Rate

Auto Mbps

Legacy Rate Sets

Rate (Mbps)

54 48 36 24 18 12 11 9 6 5.5 2 1

Supported

☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒

Basic

☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☒ ☒ ☒

MCS (Data Rate) Settings

Index

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

Enable/Disable

☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒ ☒

☐ Broadcast/Multicast Rate Limiting

Rate Limit

50 (packets per second)

Rate Limit Burst

75 (packets per second)

☐ Forced Roaming

Forced Roaming Signal

20 (Percent, Range: 20 - 60)

TSPEC Mode

Off

TSPEC Voice ACM Mode

Off

TSPEC Voice ACM Limit

20 (Percent, Range: 0 - 70)

TSPEC Video ACM Mode

Off

TSPEC Video ACM Limit

15 (Percent, Range: 0 - 70)

TSPEC AP Inactivity Timeout

30 (Sec, Range: 0 - 120, 0 Disables)

Рис. 5.34. Настройки MCS на точке доступа D-Link DWL-3600AP

В связи с тем, что существует множество схем MCS, определяющих различные скорости передачи, возникает вопрос выбора устройства 802.11n и его скорости. На рынке оборудования представлены устройства 802.11n со следующими максимальными скоростями:

- 150 Мбит/с (обозначается как N150): используется канал шириной 40 МГц, один пространственный поток, укороченный защитный интервал 400 нс, модуляция 64-QAM (номер схемы MCS7);
- 300 Мбит/с (обозначается как N300): используется канал шириной 40 МГц, два пространственных потока, укороченный защитный интервал 400 нс, модуляция 64-QAM (номер схемы MCS15);
- 450 Мбит/с (обозначается как N450): используется канал шириной 40 МГц, три пространственных потока, укороченный защитный интервал 400 нс, модуляция 64-QAM (номер схемы MCS23);
- 600 Мбит/с (обозначается как N600): используется канал шириной 40 МГц, четыре пространственных потока, укороченный защитный интервал 400 нс, модуляция 64-QAM (номер схемы MCS31).

На рис. 5.35 показаны скорости передачи 802.11n в зависимости от комбинирования различных технологий.

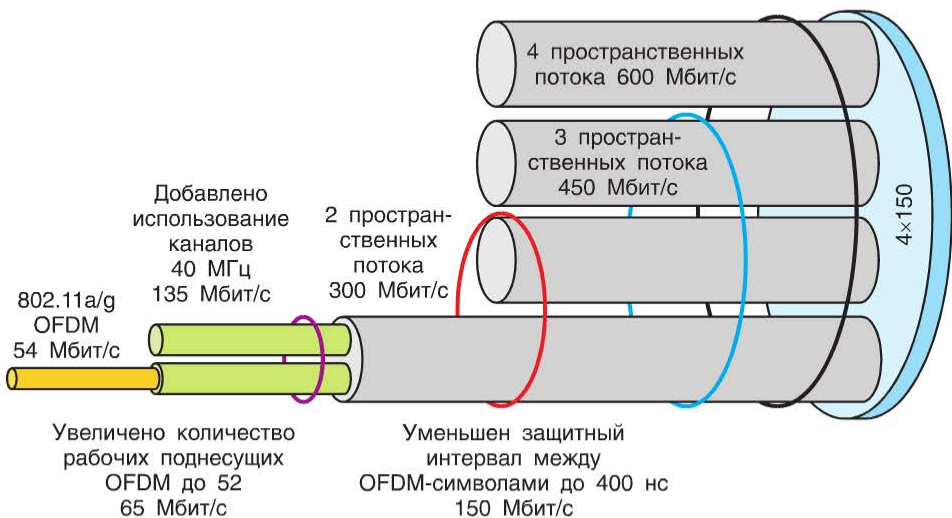


Рис. 5.35. Технологии повышения производительности 802.11n

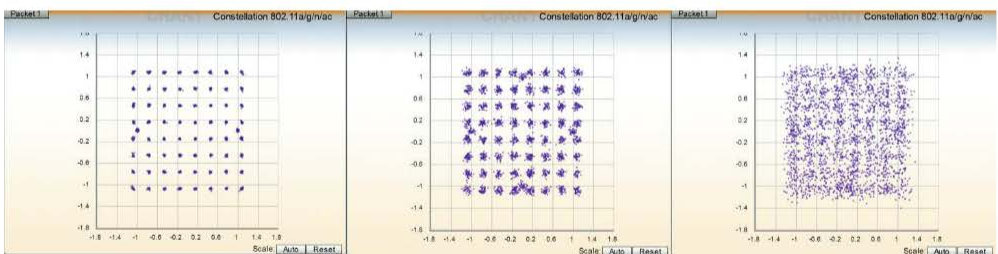


Рис. 5.36. Искажение сигнала созвездия реального сигнала под воздействием помех

При передаче данных между беспроводными устройствами сигналы подвергаются воздействию помех, что приводит к их искажениям в приемнике, которые можно оценить по искажению сигнального созвездия. Точки на сигнальном созвездии при искажении сигнала смещаются относительно их математического положения на некоторые расстояния, зависящие от интенсивности шумов и помех. При высоком уровне шумов величина смещения точек созвездия превосходит расстояние между этими точками, что приводит к ошибкам передачи, поскольку сигнал демодулируется в неверную битовую последовательность. Случай искажения сигнального созвездия для модуляции 64-QAM в реальной беспроводной системе передачи данных показан на рис. 5.36.

5.6.2. Совместимость со спецификациями 802.11a/b/g

До появления спецификации 802.11n было выпущено множество устройств, поддерживающих предыдущие спецификации — 802.11a/b/g, поэтому перед разработчиками 802.11n стояла задача обеспечения совместимости и возможности сосуществования в одном частотном диапазоне устройств 802.11n и 802.11a/b/g.

На подуровне PLCP физического уровня НТ определено три режима (три формата кадров PLCP), в которых может работать оборудование 802.11n (рис. 5.37):

- *Non-HT (Legacy) format.* Режим совместимости с оборудованием предыдущих версий. Кадры передаются в форматах канального и физического уровня спецификаций 802.11a/g, поэтому клиенты 802.11a/b/g могут взаимодействовать с точкой доступа. В этом режиме не обеспечивается поддержка специфических функций 802.11n, точка доступа должна использовать для работы только каналы шириной 20 МГц. Поддержка этого режима является обязательной;

Non-HT format



HT-greenfield format



HT-mixed format



- STF Short Training Field
- LTF Long Training Field
- SIG Signal
- GF Greenfield
- L Legacy (802.11a/b/g)
- HT High Throughput (802.11n)

Примечание: В терминологии 802.11n, L = Non-HT

Рис. 5.37. Форматы преамбул кадров подуровня PLCP физического уровня НТ

- *HT-greenfield format*. Высокоскоростной режим, в котором обеспечивается поддержка только устройств спецификации 802.11n. Кадры передаются в форматах канального и физического уровня спецификации 802.11n, в результате чего их не могут декодировать устройства старых версий. Подразумевается, что в рабочем частотном диапазоне нет клиентских устройств 802.11a/b/g и точка доступа не ожидает их подключения. Если клиентские устройства 802.11a/b/g в данном частотном диапазоне существуют, они не смогут обнаруживать кадры, отправляемые точкой доступа, и будут воспринимать их как помехи. Поддержка этого режима опциональна;

- *HT-mixed format*. Смешанный режим, в котором обеспечивается полная совместимость с оборудованием 802.11a/b/g и частичная поддержка спецификации 802.11n. К передаваемым кадрам MAC-подуровня на подуровне PLCP добавляются две преамбулы: преамбула физического уровня 802.11a/g и преамбула физического уровня HT. Благодаря этому устройства 802.11a/b/g/n могут совместно работать в одном частотном диапазоне. Поддержка этого режима является обязательной.

DIR-860L	SETUP	ADVANCED	TOOLS	STATUS
INTERNET	WIRELESS NETWORK Use this section to configure the wireless settings for your D-Link router. Please note that changes made in this section may also need to be duplicated on your wireless client. To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA and WPA2. <input type="button" value="Save Settings"/> <input type="button" value="Don't Save Settings"/>			
WIRELESS SETTINGS				
NETWORK SETTINGS				
STORAGE				
MEDIA SERVER				
IPV6				
MYDLINK SETTINGS	WIRELESS NETWORK SETTINGS <div> Wireless Band : 2.4GHz Band Enable Wireless : <input checked="" type="checkbox"/> Always <input type="button" value="New Schedule"/> Wireless Network Name : dlink-F1F8 (Also called the SSID) 802.11 Mode : Mixed 802.11n, 802.11g and 802.11b Enable Auto Channel Scan : <input type="checkbox"/> Wireless Channel : 2.412 GHz - CH 1 Transmission Rate : Best (automatic) (Mbit/s) Channel Width : 20/40 MHz(Auto) Visibility Status : <input checked="" type="radio"/> Visible <input type="radio"/> Invisible </div>			

Рис. 5.38. Настройка смешанного режима работы 802.11b/g/n и ширины канала 20/40 МГц на маршрутизаторе D-Link DIR-860

Следует отметить, что только в режиме HT-greenfield можно в полной мере воспользоваться преимуществами высокой скорости, достигнутыми в спецификации 802.11n. Однако обычно в точках доступа или беспроводных маршрутизаторах 802.11n настраивается смешанный режим работы (рис. 5.38, 5.39). Режим позволяет использовать каналы шириной 40 МГц, но при этом

сохраняет совместимость с оборудованием 802.11a/b/g, пересылая широко-вещательные и неагрегированные кадры через первичный канал шириной 20 МГц. Все передачи от клиентов 802.11a/b/g также выполняются через первичный канал шириной 20 МГц. Для таких операций в устройствах 802.11n используется обозначение «20/40 MHz».

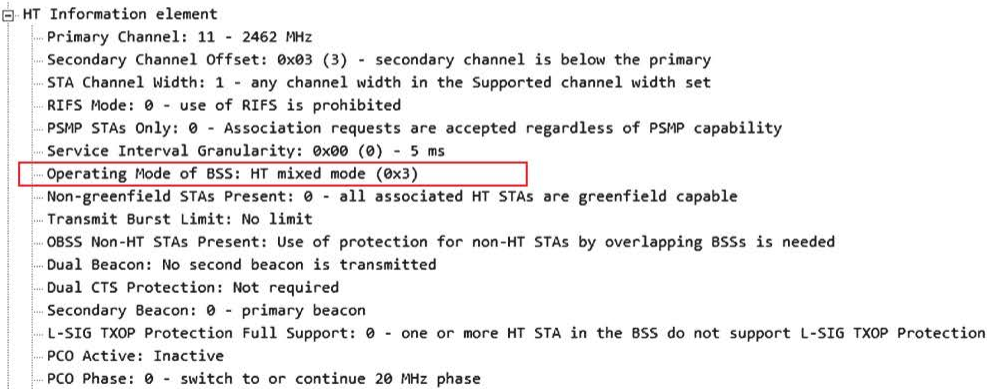


Рис. 5.39. Информация о режиме работы беспроводной сети в кадре Probe Response

5.6.3. Структура физического интерфейса 802.11n

Передатчик, осуществляющий отправку данных в форматах HT-greenfield и HT-mixed, включает в себя следующие блоки (рис. 5.40).

1. *Скремблер (Scrambler)* — принимает входной информационный битовый поток и за счет перестановки битов уменьшает вероятность возникновения длинных последовательностей 0 и 1, что повышает надежность связи.

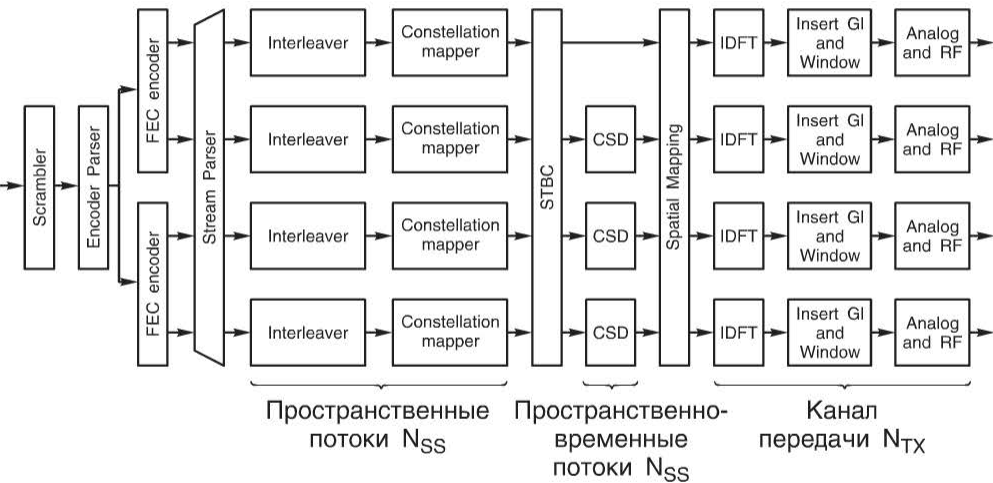


Рис. 5.40. Блок-схема передатчика 802.11n

2. *Кодеры FEC (FEC encoder)* — кодируют данные с целью выявления ошибок передачи с помощью либо сверточных ВСС, либо LDPC-кодов. Перед кодерами находится блок выбора вида кода (*Encoder Parser*).

3. *Потоковый анализатор (Stream Parser)* — разбивает данные, полученные от кодеров, на пространственные потоки.

4. *Устройства чередования (Interleaver)* — изменяют порядок битов каждого пространственного потока, получаемых после кодирования, для предотвращения появления длинных последовательностей 0 или 1. Устройства используются только для ВСС-кодов.

5. *Демультимплексоры (Constellation mapper)* — разбивают входную последовательность на N параллельных потоков по k бит, где N — число поднесущих OFDM-символа, k — число битов для отображения одного символа на одной из поднесущих (число модулируемых битов). Модуляция заключается в том, что каждые k бит (от 1 до 6 в зависимости от выбранной схемы модуляции и кодирования MCS) по определенному закону заменяются одним импульсом с конкретными амплитудой и фазой. Такое преобразование последовательности k бит удобно изображать на плоскости в виде сигнального созвездия. На рис. 5.41 показано сигнальное созвездие для модуляции QAM-16. Как видно из рисунка, последовательности битов 1100 соответствует импульс (1 бит) с амплитудой 25 % от максимума и фазой 225°. Таким образом, модуляция QAM-16 заменяет 4 информационных бита на 1 бит, что приводит к увеличению скорости передачи в 4 раза.

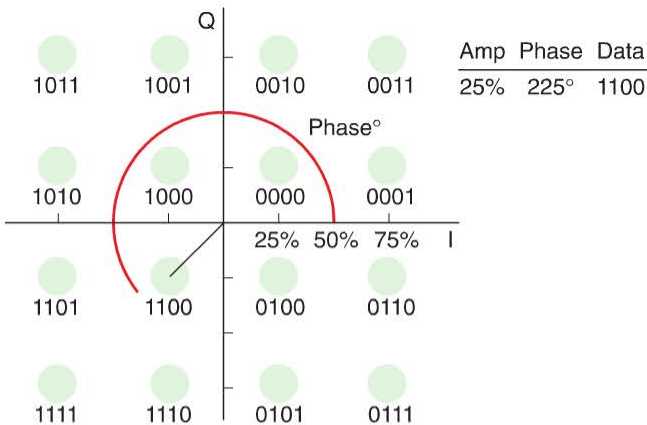


Рис. 5.41. Сигнальное созвездие QAM-16

6. *Кодер STBC (STBC encoder)* — распределяет точки сигнального созвездия одного пространственного потока между множеством радиочастотных трактов, формируя из одного пространственного потока множество пространственно-временных потоков с помощью пространственно-временного кодирования.

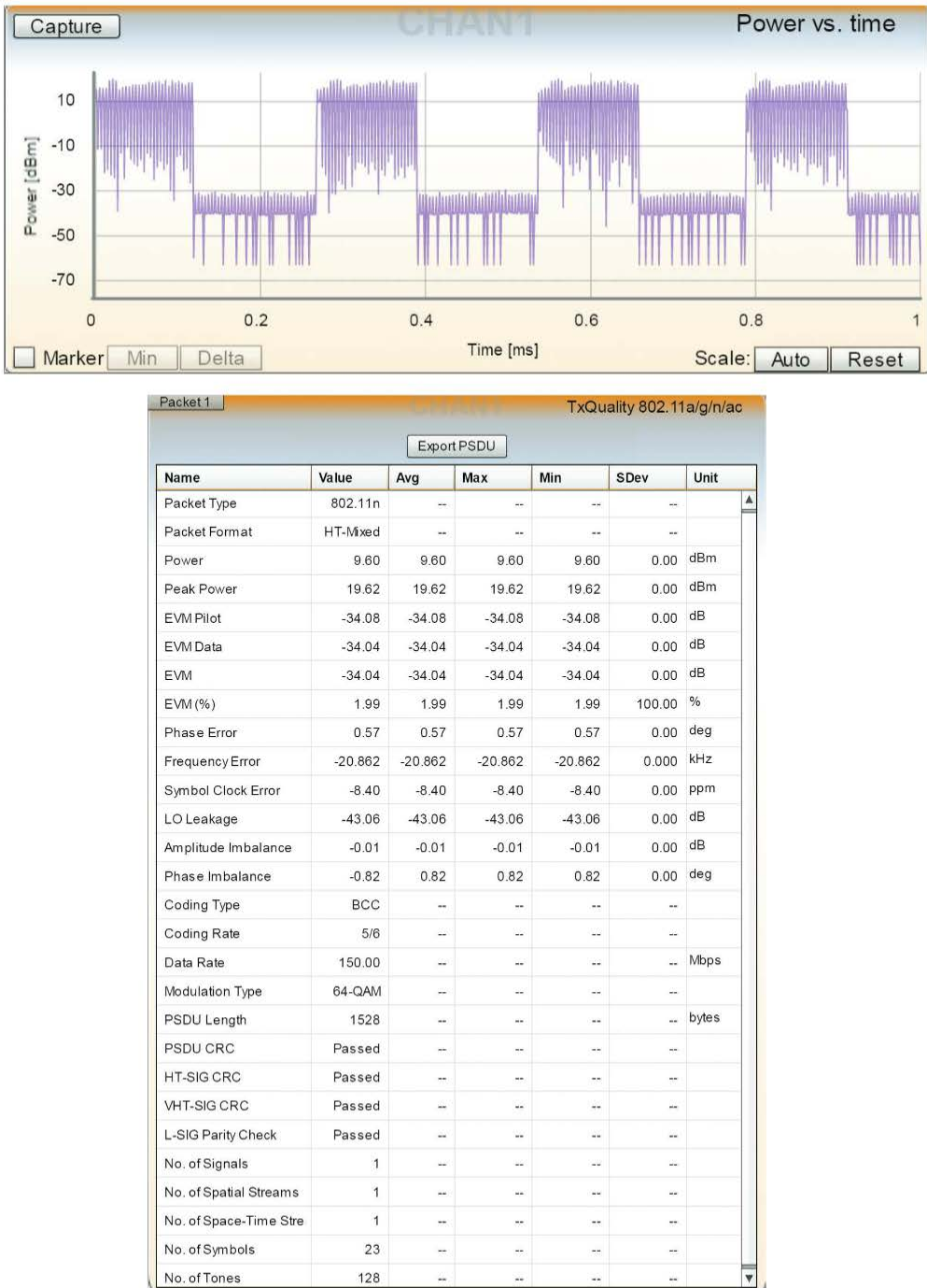


Рис. 5.42. Реальный сигнал стандарта 802.11n во времени и его измеренные параметры

7. *Блоки пространственного преобразователя (Spatial Mapping)* — выполняют привязку пространственно-временных потоков к трактам передачи. Существует три формы привязки: *непосредственная привязка (direct mapping)*, которая привязывает точки модуляционного созвездия каждого пространственно-временного потока к одному тракту передачи; *пространственное расширение (spatial expansion)*, при котором точки сигнального созвездия всех пространственно-временных потоков привязываются ко всем трактам передачи; *формирование луча (beamforming)*, при котором все пространственно-временные потоки распределяются по трактам передачи таким образом, чтобы энергия была сфокусирована в определенном направлении.

8. *Блоки обратного преобразования Фурье (Inverse discrete Fourier transform, IDFT)* — преобразуют сигнал из частотного представления во временное, формируя тем самым OFDM-символы. Каждый OFDM-символ представляет собой импульс, содержащий n поднесущих.

9. *Блоки вставки циклического сдвига (Cyclic shift, CSD)* — добавляют небольшую фазовую задержку для предотвращения случайного формирования диаграммы направленности. Эти блоки могут находиться до блока IDFT или после него.

10. *Блоки вставки защитного интервала (GI Insertion)* — добавляют к началу OFDM-символа циклическое повторение его окончания, защищая сигнал от межсимвольной интерференции.

11. *Радиочастотные модуляторы и усилители мощности* — переносят спектр сигнала на несущую частоту диапазона 2,4 ГГц или 5 ГГц и усиливают его.

12. *Антенны* — осуществляют излучение сигнала в окружающее пространство.

Приемник физического интерфейса 802.11n построен по аналогичной схеме с несколькими отличиями. Вместо усилителя мощности используется малошумящий усилитель, обладающий невысоким усилением, но и не искажающий входной сигнал. Также на входе приемника производится автоматическая регулировка усиления для уменьшения ошибок передачи. Далее после демодуляции осуществляется частотная коррекция для уменьшения ошибок, возникающих вследствие сдвига частоты передаваемого сигнала. Остальные операции точно такие же, как и в передатчике, но выполняемые в обратном порядке.

На рис. 5.42 показан реальный сигнал стандарта 802.11n маршрутизатора D-Link DIR-825/ACF длительностью 1 мс, измеренный на тестовом оборудовании компании D-Link.

5.6.4. Технологии повышения производительности на MAC-подуровне 802.11n

Спецификация 802.11n включает несколько технологий MAC-подуровня, позволяющих повысить производительность передачи данных.

Агрегация кадров

При передаче каждого кадра точка доступа или клиент соревнуются за доступ к среде. В результате теряется время, которое можно было бы потратить на передачу трафика. Спецификация 802.11n включает механизмы аг-

регации кадров, которые позволяют уменьшить количество соревнований за среду передачи. Благодаря агрегации кадров на MAC-подуровне станция с большим количеством кадров для передачи может объединить их в один агрегированный кадр. Таким образом, уменьшается количество передаваемой служебной информации и уменьшается общее время состязания за доступ к среде передачи.

Существует два разных метода агрегации, известных как *Aggregated MAC Service Data Unit (A-MSDU, агрегированный блок данных сервиса MAC)* и *Aggregated MAC Protocol Data Unit (A-MPDU, агрегированный блок данных протокола MAC)* (рис. 5.43).

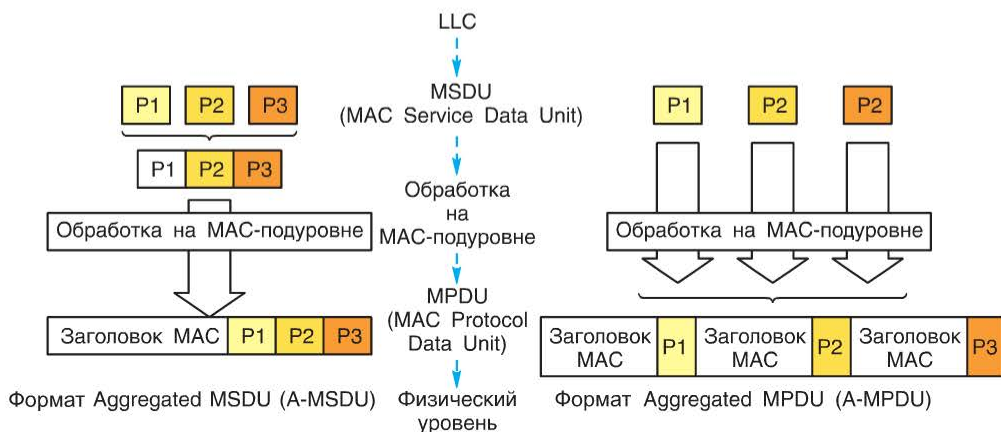


Рис. 5.43. Механизмы агрегации A-MSDU и A-MPDU

Формат A-MSDU позволяет объединить множество кадров MSDU, полученных от вышележащего уровня, и передать их как единый (нефрагментированный) кадр MAC-подуровня (MPDU). Каждый оригинальный MSDU становится подкадром внутри агрегированного кадра. Использовать этот метод агрегации можно только для MSDU с одинаковым приоритетом и одинаковыми адресами источника и получателя. Агрегированный кадр A-MSDU содержит один заголовок, его максимальный размер составляет 3839 или 7935 байт в зависимости от возможностей станции плюс накладные расходы на шифрование. Если к данным применяется шифрование, то шифруется весь агрегированный кадр.

Альтернативный метод, формат A-MPDU, применяется после добавления к каждому кадру MSDU заголовка MAC-подуровня и формирования MPDU. A-MPDU состоит из последовательности одного или нескольких подкадров (*subframe*) A-MPDU, предназначенных одной принимающей станции, которые передаются через физический уровень как единый блок данных. Каждый подкадр A-MPDU состоит из разделителя MPDU (*MPDU delimiter*), за которым

следует MPDU. Целью использования разделителя MPDU является определение местоположения соответствующего MPDU в агрегированном кадре. Максимальная длина агрегированного кадра A-MPDU равна 65535 байт. Каждый индивидуальный MPDU внутри объединенного блока данных шифруется и дешифруется независимо от других. Поскольку при использовании этого метода за один раз передается группа MPDU, то невозможно выполнить подтверждение приема каждого переданного одноадресного кадра, поэтому формат A-MPDU используется совместно с функцией блочного подтверждения (*Block Acknowledgement*).

Блочное подтверждение

MAC-подуровень оригинального стандарта 802.11 требует получения подтверждений для каждого переданного одноадресного кадра. Передача считается незавершенной пока передатчиком не получено подтверждение.

Появившееся в 2005 году дополнение к стандарту IEEE 802.11e, определяющее набор функций для обеспечения качества обслуживания в беспроводных сетях, дополнительно к одиночным подтверждениям добавило механизм *блочных подтверждений* (*Block Acknowledgement, Block Ack*), позволяющий передатчику передавать поток кадров и получать от приемника за один раз все подтверждения, объединенные в едином кадре. Этот механизм также используется в 802.11n.

Благодаря объединению подтверждений в один кадр уменьшается количество кадров ACK, которые получатель должен послать отправителю, и, следовательно, повышается эффективность использования канала. Блочные подтверждения могут использоваться как для подтверждения получения A-MPDU, так и для подтверждения получения группы кадров одним приемником (рис. 5.44).



Рис. 5.44. Блочные подтверждения

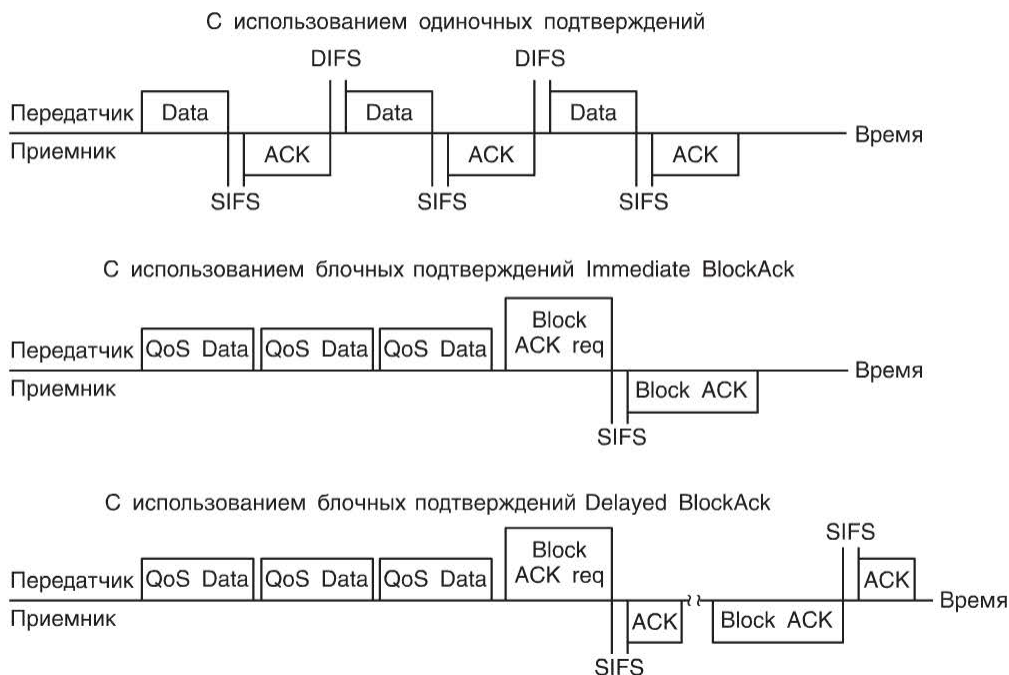


Рис. 5.45. Сравнение методов подтверждения приема кадров

Существует две формы блочных подтверждений: *мгновенные* (*Immediate Block Ack*) и *с задержкой* (*Delayed Block Ack*) (рис. 5.45). При использовании мгновенных блочных подтверждений отправитель посылает поток кадров и ожидает получение подтверждения немедленно. При использовании блочных подтверждений с задержкой получатель может отправить подтверждение позже.

5.6.5. Механизмы защиты 802.11n при работе в сети с устройствами 802.11a/b/g

При появлении новых беспроводных технологий в них зачастую реализуют механизмы передачи, отличные от используемых в устройствах предыдущих спецификаций. Старые устройства не могут правильно интерпретировать кадры новых устройств, работающих в том же частотном диапазоне, в результате чего может возникать интерференция сигналов. При появлении спецификации 802.11g, использовавшей на физическом уровне модуляцию OFDM, устройства 802.11b не могли декодировать кадры, отправляемые новыми устройствами. В результате возникла необходимость в механизмах, которые позволяли бы одновременно работать в одной сети устройствам 802.11b и 802.11g. Эти механизмы были стандартизированы и получили название *механизмов защиты* (*protection*).

Прежде чем начать передачу в формате 802.11g, устройство должно гарантировать, что станции 802.11b отложат доступ к беспроводной среде. Для этого в качестве механизмов защиты спецификация 802.11g использует ме-

тоды RTS/CTS и CTS-to-self на MAC-подуровне, которые являются расширением метода доступа DCF. Таким образом, методы RTS/CTS и CTS-to-self обеспечивают защиту и позволяют решить проблему «скрытого узла». Спецификация 802.11n также использует методы RTS/CTS и CTS-to-self в качестве механизмов защиты передаваемых кадров 802.11n на MAC-подуровне. Используя метод CTS-to-self, точка доступа 802.11n при наличии данных для передачи может отправить кадр CTS в формате non-HT. В поле адреса станции назначения этого кадра указывается ее собственный MAC-адрес, а в поле «Длительность» — период времени, на который все остальные станции должны воздержаться от доступа к среде. Метод RTS/CTS расширен процедурой dual CTS: клиент 802.11n отправляет точке доступа кадр RTS в формате HT, а точка доступа отвечает двумя кадрами CTS — в формате HT и в формате non-HT. Таким образом, в результате обмена кадрами RTS/CTS с точкой доступа клиент 802.11n сможет зарезервировать канал, а устройства предыдущих версий правильно установить свои векторы NAV и отложить передачу (рис. 5.46).

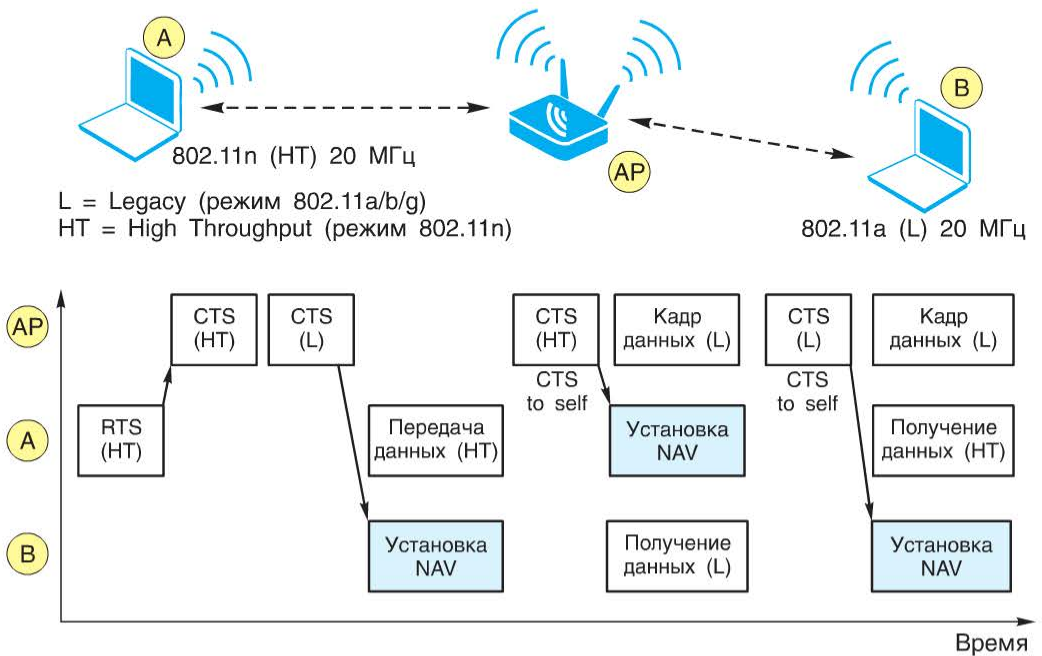


Рис. 5.46. Методы защиты на MAC-подуровне

В дополнение к методам защиты на MAC-подуровне в 802.11n был добавлен механизм защиты на физическом уровне: *L-SIG TXOP protection*. Этот метод является альтернативным и не требует обмена контрольными кадрами, значительно снижающими пропускную способность сети. При работе устройств 802.11n в смешанном режиме требуется, чтобы кадр PLCP имел две преамбулы: преамбулу физического уровня спецификаций 802.11a/g

и преамбулу физического уровня HT (см. рис. 5.37). Наличие преамбулы физического уровня спецификаций 802.11a/g в кадре PLCP позволяет устройствам определить начало передачи, вычислить ее длительность с помощью поля L-SIG и установить свои векторы NAV. Таким образом, устройства 802.11a/b/g могут избежать передачи кадров одновременно с устройствами 802.11n.

Правила защиты

Рассмотрим использование описанных выше механизмов защиты. Устройства 802.11n объявляют о требуемом типе защиты, используя информационный элемент HT кадров Beacon или Probe Response (рис. 5.47).

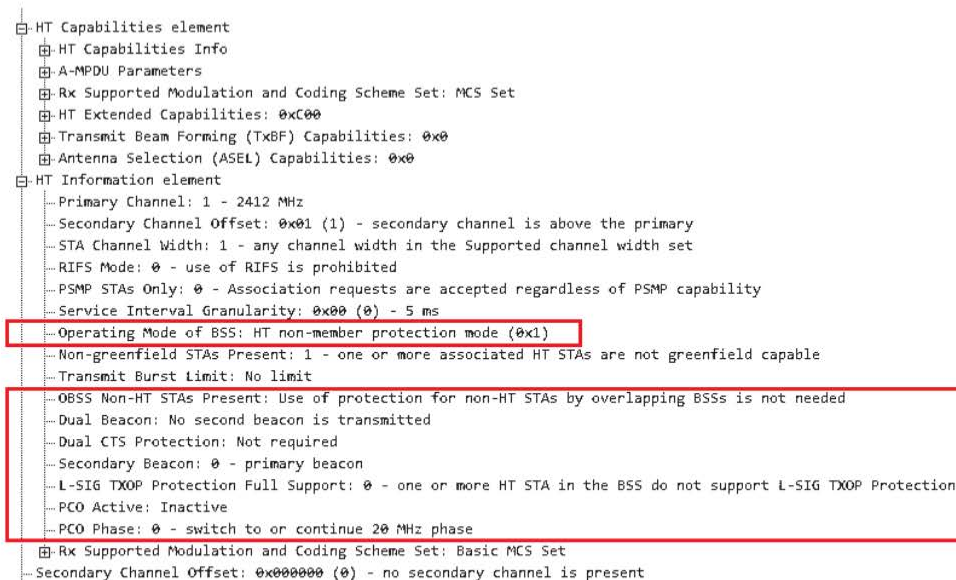


Рис. 5.47. Информационный элемент HT кадра Beacon

Всего в спецификации 802.11n определено четыре режима защиты, и в каждой сети выбирается один из них (рис. 5.48, 5.49):

- *No protection* (без защиты) — не определяет использования специальных правил передачи. Этот режим устанавливается в том случае, когда сеть состоит только из устройств 802.11n;

- *Non-member protection* (защита от не членов BSS) — предполагает защиту от устройств 802.11a/g, которые не являются членами сети, состоящей только из устройств 802.11n. Этот режим применяется, когда необходимо предотвратить интерференцию сети 802.11n с соседними сетями, работающими на том же канале и содержащими устройства предыдущих спецификаций;

- *20 MHz protection* (защита при использовании канала 20 МГц) — используется в том случае, если в сети, где все станции являются устройствами

802.11n и настроены для работы на каналах шириной 20/40 МГц, существует по крайней мере одна станция 802.11n, использующая для работы канал шириной 20 МГц;

- *Non-HT mixed* (смешанный режим) — при работе в этом режиме кадр PLCP передается с двумя преамбулами: преамбулой физического уровня 802.11a/g, содержащей поле L-SIG, и преамбулой физического уровня 802.11n.

```

HT Information element
...Primary Channel: 8 - 2447 MHz
...Secondary Channel Offset: 0x01 (1) - secondary channel is above the primary
...STA Channel Width: 1 - any channel width in the Supported channel width set
...RIFS Mode: 0 - use of RIFS is prohibited
...PSMP STAs Only: 0 - Association requests are accepted regardless of PSMP capability
...Service Interval Granularity: 0x00 (0) - 5 ms
...Operating Mode of BSS: Only HT STAs in the BSS, however, there exists at least one 20 MHz STA (0x2)
...Non-greenfield STAs Present: 1 - one or more associated HT STAs are not greenfield capable
...Transmit Burst Limit: No limit
...OBSS Non-HT STAs Present: Use of protection for non-HT STAs by overlapping BSSs is not needed
...Dual Beacon: No second beacon is transmitted
...Dual CTS Protection: Not required
...Secondary Beacon: 0 - primary beacon
...L-SIG TXOP Protection Full Support: 0 - one or more HT STA in the BSS do not support L-SIG TXOP Protection
...PCO Active: Inactive
...PCO Phase: 0 - switch to or continue 20 MHz phase
[Rx Supported Modulation and Coding Scheme Set: Basic MCS Set

```

Рис. 5.48. Информация о режиме работы BSS в кадре Beacon

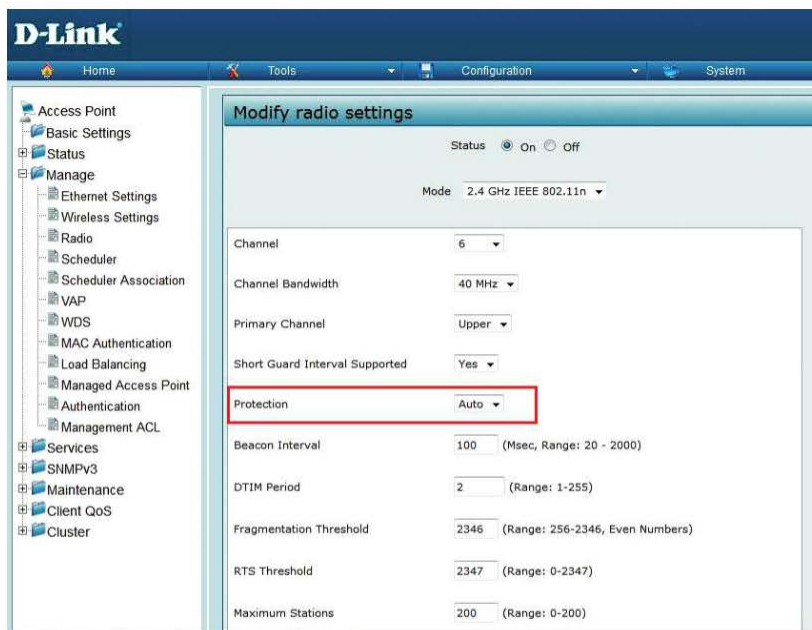


Рис. 5.49. Настройка защиты на точке доступа D-Link DWL-3600AP

5.6.6. Механизмы сосуществования при использовании каналов 20/40 МГц

Точка доступа 802.11n может быть настроена для работы с каналами шириной только 20 МГц, только 40 МГц или 20/40 МГц (рис. 5.50). Если устройство настроено для работы с каналами шириной 40 МГц, должны поддерживаться механизмы, позволяющие сетям с каналами 20 и 40 МГц сосуществовать в одном частотном диапазоне. При этом точка доступа должна автоматически переходить на использование канала 20 МГц в случае обнаружения интерференции сигналов.

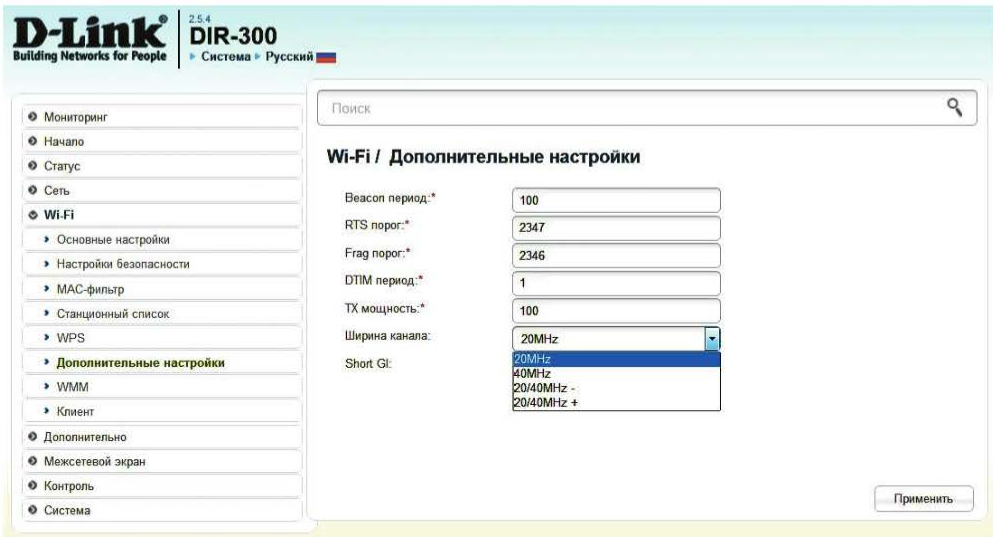


Рис. 5.50. Настройка ширины каналов на маршрутизаторе D-Link DIR-300

Устройства 802.11n должны обмениваться информацией об используемой ширине канала. Эта информация указывается в элементе HT Capabilities кадра Beacon или Probe Response (рис. 5.51).

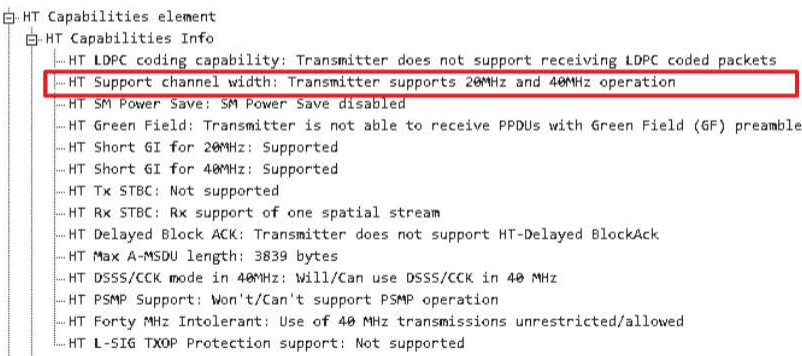


Рис. 5.51. Информация о ширине канала в кадре Beacon

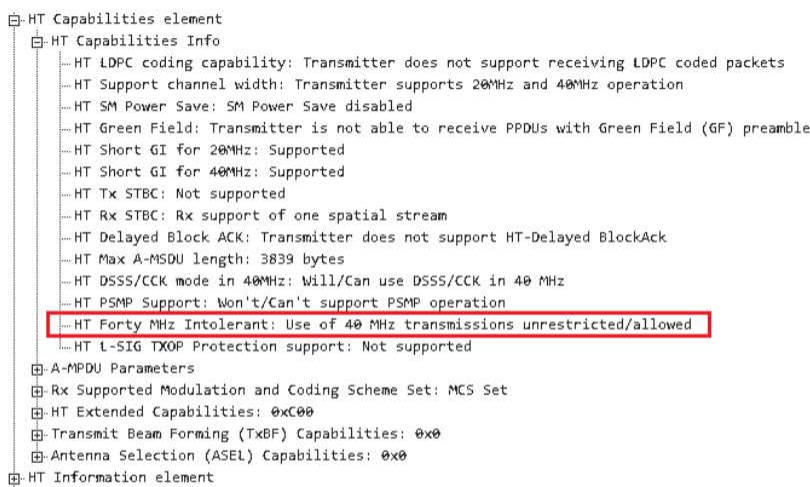


Рис. 5.52. Поле Forty MHz Intolerant в кадре Beacon

В спецификации 802.11n существуют правила, определяющие механизмы сосуществования в одном частотном диапазоне каналов шириной 20 и 40 МГц. Прежде чем начать использовать канал шириной 40 МГц, точка доступа 802.11n должна выполнить сканирование всех каналов, чтобы найти все сети, первичные каналы которых перекрываются с ее вторичным каналом. Если такие сети найдены, точка доступа должна переключиться на работу в первичном канале шириной 20 МГц. Далее она может изменить номер первичного канала или обоих (первичного и вторичного) каналов.

В диапазоне 5 ГГц точка доступа не может начать использовать канал шириной 40 МГц, если ее вторичный канал перекрывается с первичным каналом другой сети. В этом случае точка доступа должна выбрать первичный и вторичный каналы, идентичные каналам другой сети.

Если точка доступа или клиент 802.11n получили кадр Beacon, Probe Request или Probe Response, содержащий в поле Forty MHz Intolerant элемента HT Capabilities (рис. 5.52) значение 1, то они должны переключиться на использование первичного канала шириной 20 МГц. Механизм, сигнализирующий о запрете использования канала шириной 40 МГц (Signaling 40 MHz intolerance), позволяет точкам доступа или клиентским станциям, работающим в диапазоне 2,4 ГГц на канале шириной 20 МГц, сообщать о том, что они запрещают использовать каналы 40 МГц членам перекрывающихся с ними сетей или другим членам этой же сети. Другими словами, они сигнализируют о том, что соседние с ними устройства должны работать только на каналах шириной 20 МГц. В диапазоне 5 ГГц существует достаточное количество неперекрывающихся каналов, поэтому этот механизм не используется.

При переходе точки доступа на использование другого набора каналов или изменении ширины используемого канала она должна иметь возможность

сообщить об этом ассоциированным с ней клиентам. Для этого она включает в кадр Beacon или Probe Response элемент Extended Channel Switch Announcement, содержащий новые данные, или отправляет специальный кадр Extended Channel Switch Announcement. Как только клиенты получают это извещение, они выполняют необходимые изменения и уведомляют об этом точку доступа, отправляя кадр Beacon или Probe Response с установленным элементом Extended Channel Switch Announcement или кадр Extended Channel Switch Announcement.

Операция фазового совместного существования (Phased coexistence operation, PCO) является дополнительным механизмом обеспечения работы в одной сети устройств, использующих каналы шириной 20 и 40 МГц. Точка доступа, у которой активирована эта функция, делит время между операциями в первичном канале 20 МГц и операциями в канале 40 МГц.

Правила доступа к каналам 40 МГц

Перед тем как начать передачу кадра в канале шириной 40 МГц, беспроводная станция 802.11n должна гарантировать, что первичный и вторичный каналы свободны. Для этого она полностью выполняет в первичном канале функцию *clear channel assessment* (CCA), которая определяет текущее состояние использования среды передачи. Все временные интервалы, которые требуется выдержать, прежде чем получить доступ к среде, применяются только к первичному каналу. Вторичный канал должен быть свободен в течение времени, требуемого первичному каналу для выполнения CCA с последующим ожиданием окончания интервала PIFS или DIFS, прежде чем он станет использоваться как часть канала 40 МГц. Если вторичный канал оказался занят на более продолжительное время, станция 802.11n может начать передачу только в первичном канале или попытаться снова получить доступ к среде. Для определения занятости вторичного канала в нем выполняется функция CCA, но в урезанном варианте.

Виртуальный механизм контроля несущей, который выполняется с помощью вектора сетевого распределения (NAV), применяется только в первичном канале. Другими словами, все кадры, приводящие к обновлению векторов NAV устройств, передаются только в первичном канале.

5.7. Спецификация IEEE 802.11ac

В 2013 г. вышла спецификация 802.11ac, которая позволяет приблизить скорости беспроводных устройств к скоростям проводного оборудования. По сравнению с 802.11n в нее внесены изменения как на физическом, так и на MAC-подуровне. Появился новый физический уровень с очень высокой производительностью (*Very High Throughput, VHT*) для систем OFDM (VHT PHY), определяющий передачу на скорости до 6,93 Гбит/с и поддерживающий работу только в диапазоне 5 ГГц.

Спецификация 802.11ac, по сути, является эволюцией спецификации 802.11n: в ней расширены многие значимые технологии физического уровня

и MAC-подуровня 802.11n. В дополнение к однопользовательской форме MIMO в 802.11ac появилась многопользовательская форма MIMO (Multi-User MIMO, MU-MIMO), которая позволяет точке доступа одновременно передавать данные множеству клиентов. Сравнение основных функций 802.11n и 802.11ac и приведено в табл. 5.9.

Таблица 5.9. Сравнение 802.11n и 802.11ac

Спецификация 802.11n	Спецификация 802.11ac
Каналы шириной 20 и 40 МГц	Каналы шириной 20, 40, 80, 160 и 80+80 МГц
Работа в диапазонах 2,4 и/или 5 ГГц	Работа только в диапазоне 5 ГГц
Модуляции BPSK, QPSK, 16-QAM, 64-QAM	Модуляции BPSK, QPSK, 16-QAM 64-QAM, 256-QAM
До четырех пространственных потоков	До восьми пространственных потоков на точках доступа и до четырех пространственных потоков на клиентских устройствах
Максимальная скорость передачи 600 Мбит/с	Максимальная скорость передачи 6933 Мбит/с
Несколько типов оценки канала функции Beamforming	Поддерживается только метод Null Data Packet (NDP) точной оценки канала функции Beamforming
Однопользовательская форма MIMO	Одно- и многопользовательская формы MIMO
Улучшения MAC-подуровня (A-MSDU, A-MPDU)	Аналогичные улучшения MAC-подуровня с некоторыми расширениями для высоких скоростей

В отличие от 802.11n устройства спецификации 802.11ac используют только диапазон 5 ГГц и не доступны в диапазоне 2,4 ГГц, поскольку спектр диапазона 2,4 ГГц сильно зашумлен по сравнению с диапазоном 5 ГГц. Кроме того, значительное увеличение скорости в спецификации 802.11ac достигнуто за счет увеличения ширины каналов (дополнительно к каналам шириной 20 и 40 МГц в 802.11ac определено использование каналов шириной 80 и 160 МГц). С учетом доступного для использования спектра в диапазоне 2,4 ГГц выделить в нем канал шириной 160 МГц невозможно. Поэтому спецификация 802.11n является последней спецификацией для диапазона 2,4 ГГц, а высокоскоростная спецификация 802.11ac работает только в диапазоне 5 ГГц, так как его доступный для использования спектр значительно шире.

В 802.11ac добавлена поддержка модуляции 256-QAM, что позволяет значительно повысить скорости передачи.

Если сравнивать точку доступа с поддержкой спецификации 802.11n и точку доступа с поддержкой 802.11ac, то последняя может задействовать до

восьми пространственных потоков. Для клиентского устройства определено использование до четырех потоков. Избыточные пространственные потоки точка доступа может использовать для одновременной передачи данных сразу нескольким клиентам.

Также по сравнению с 802.11n в 802.11ac значительно упрощена функция Beamforming: в 802.11n было определено несколько вариантов реализации этой функции и для ее использования в сети требуется одинаковая реализация этой функции на всех взаимодействующих устройствах. Чтобы избежать этой проблемы в спецификации 802.11ac определен только один метод реализации функции Beamforming, называемый *Null Data Packet (NDP) sounding*.

5.7.1. Технологии физического уровня 802.11ac

Спецификация 802.11ac определяет физический уровень с очень высокой производительностью для систем OFDM (VHT PHY). Он основан на физическом уровне HT PHY, который, в свою очередь, основан на физическом уровне OFDM. В связи с этим оборудование 802.11ac обратно совместимо с оборудованием 802.11a и 802.11n при работе в диапазоне 5 ГГц. Физический уровень VHT PHY расширяет максимальное количество пространственно-временных потоков до восьми и поддерживает *нисходящие многопользовательские передачи (downlink multi-user (MU) transmission)*. При нисходящей многопользовательской передаче поддерживается до четырех пользователей, каждый из которых поддерживает до четырех пространственно-временных потоков. При этом суммарное количество потоков не может превышать восьми.

Обязательными функциями VHT PHY являются:

- использование непрерывных каналов шириной 20, 40 и 80 МГц;
- поддержка передачи и приема в формате Non-HT для всех поддерживаемых в VHT PHY размеров каналов;
- поддержка передачи и приема в форматах HT-mixed, VHT;
- поддержка передачи и приема одного пространственного потока для всех, поддерживаемых в VHT PHY размеров каналов (схемы VHT-MCS от 0 до 7);
- поддержка двоичного сверточного кодирования.

Опциональными функциями VHT PHY являются:

- использование непрерывных каналов шириной 160 МГц;
- использование прерывающихся каналов шириной 80+80 МГц;
- формирование диаграммы направленности передатчика (метод NDP);
- использование кодирования STBC при приеме и передаче;
- использование кодирования LDPC при приеме и передаче;
- использование укороченного защитного интервала (Short GI);
- поддержка передачи и приема кадров при многопользовательской передаче.

Ширина каналов

Значительное повышение скорости в спецификации 802.11ac достигнуто за счет увеличения ширины каналов. В 802.11ac сохранилось использование каналов шириной 20 и 40 МГц (как в 802.11a и 802.11n) и добавилась под-

держка каналов шириной 80 и 160 МГц в диапазоне 5 ГГц (поддержка каналов шириной 160 МГц является опциональной). Подход к получению каналов разной ширины аналогичен подходу, используемому в 802.11n. Для получения канала шириной 40 МГц объединяются два соседних канала шириной 20 МГц, для получения канала шириной 80 МГц объединяются два соседних канала шириной 40 МГц, канал шириной 160 МГц получается из пары каналов шириной 80 МГц. При этом для создания такого канала могут использоваться как два соседних канала шириной 80 МГц (создается непрерывный канал шириной 160 МГц), так и два отдельных (несоседних) канала шириной 80 МГц (создается прерывающийся канал 80+80 МГц). Возможность использования двух несоседних каналов шириной 80 МГц добавлена в 802.11ac с целью избежания интерференции и эффективного использования спектра, так как не всегда возможно найти непрерывный блок спектра шириной 160 МГц. При этом каждый из каналов 80 МГц должен быть непрерывным.

Спектральные маски каналов 802.11ac имеют такую же форму, как спектральные маски 802.11a и 802.11n, и отличаются только шириной (рис. 5.53).

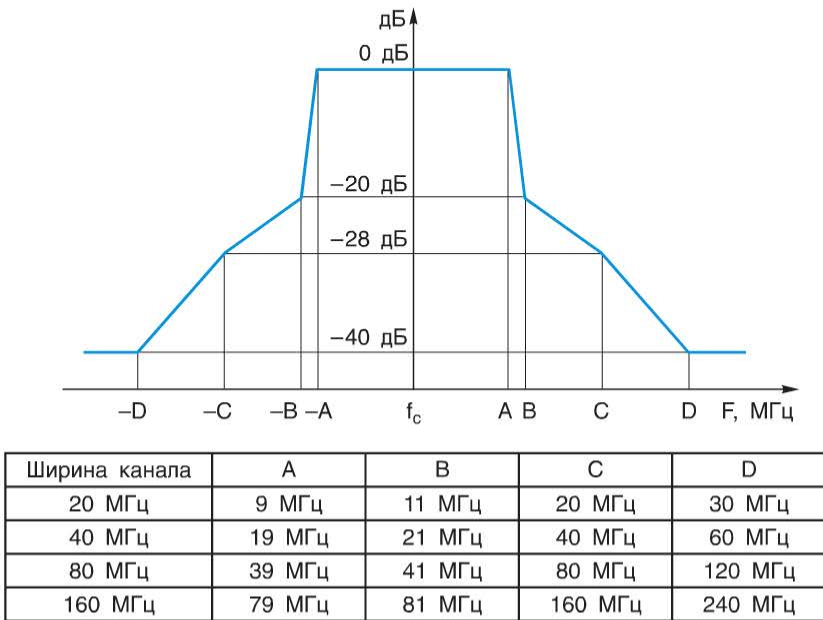


Рис. 5.53. Спектральные маски спецификации 802.11ac для каналов 20, 40, 80 и 160 МГц

На рис. 5.54 показана спектральная маска канала 80 МГц спецификации 802.11ac и спектр реального сигнала в диапазоне 5 ГГц. Как видно из рисунка, спектр сигнала искажен вследствие влияния шумов передатчика и неидеальности частотных характеристик тракта передачи сигнала.

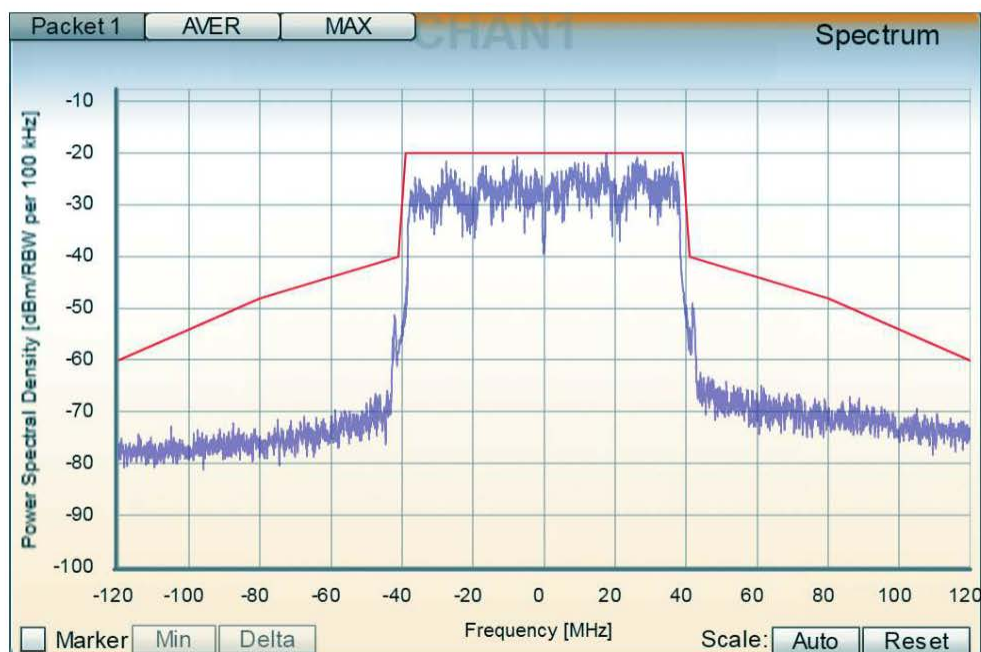


Рис. 5.54. Спектральная маска 802.11ac для канала 80 МГц и спектр реального сигнала в диапазоне 5 ГГц

По сравнению со спецификацией 802.11n количество поднесущих в каналах шириной 20 и 40 МГц не изменилось: в канале 20 МГц используется 56 поднесущих (52 рабочие и 4 служебные); в канале 40 МГц — 114 поднесущих (108 рабочих и 6 служебных); в каналах 80 МГц и 80+80 МГц — 242 поднесущих (234 рабочих и 8 служебных); в канале 160 МГц — 484 поднесущих (468 рабочих и 16 служебных) (рис. 5.55).

Для оборудования спецификации 802.11ac в России выделены две полосы в диапазоне 5 ГГц: 5150–5350 МГц и 5650–6425 МГц.

В полосе 5150–5350 МГц доступно для использования 8 каналов шириной 20 МГц, 4 канала шириной 40 МГц, 2 канала шириной 80 МГц, 1 канал шириной 160 МГц (рис. 5.56). В полосе 5650–6425 МГц доступно для использования 38 каналов шириной 20 МГц, 19 каналов шириной 40 МГц, 9 каналов шириной 80 МГц, 4 канала шириной 160 МГц.

Для каналов шириной 40 МГц и выше 802.11ac по аналогии с 802.11n использует терминологию «основной» или «первичный» (*primary*) и «вторичный» (*secondary* или *non-primary*) канал. Первичный канал — это канал, который используется для передачи кадров в своей собственной полосе частот. Вторичный канал — это канал, ассоциированный с первичным и служащий для формирования более широкого канала. Одной из причин употребления терминов «первичный» и «вторичный» является организация использования одного и того же частотного диапазона множеством беспроводных сетей.

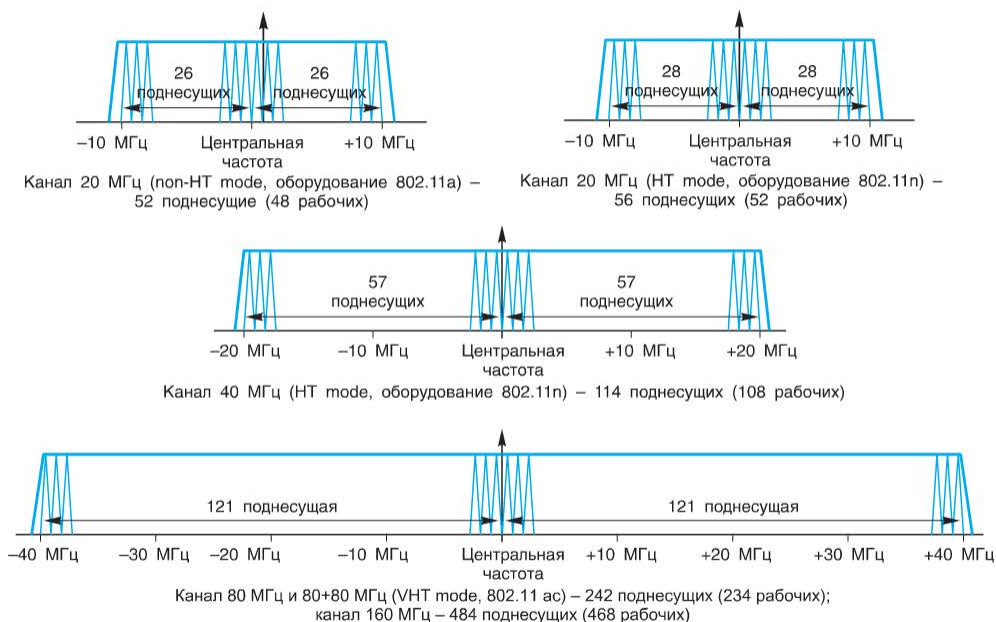


Рис. 5.55. Количество поднесущих OFDM

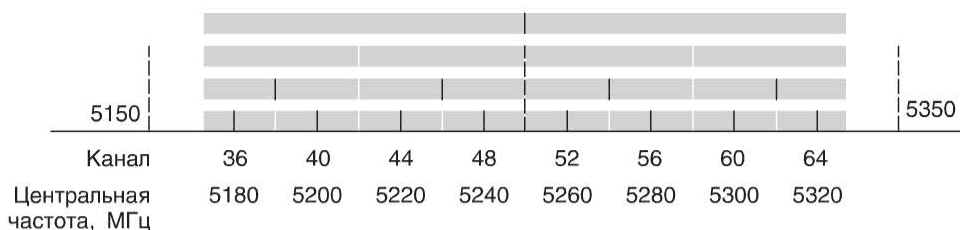


Рис. 5.56. Каналы 802.11ac, определенные в полосе частот 5150–5350 МГц

Аналогично спецификации 802.11n канал шириной 40 МГц состоит из первичного канала 20 МГц и вторичного канала 20 МГц. Канал 80 МГц состоит из первичного канала 40 МГц (который включает первичный канал 20 МГц) и вторичного канала 40 МГц. Это же относится и к каналам 160 МГц и 80+80 МГц: они состоят из первичного канала 80 МГц и вторичного канала 80 МГц (рис. 5.57).

Во всех случаях первичный канал служит для обнаружения несущей, что позволяет гарантировать, что ни одно из устройств не ведет передачу. Первичные каналы 40 и 80 МГц должны включать один первичный канал (подканал) 20 МГц, что необходимо для обеспечения сосуществования в одном частотном диапазоне устройств разных спецификаций и совместимости с устройствами предыдущих стандартов.

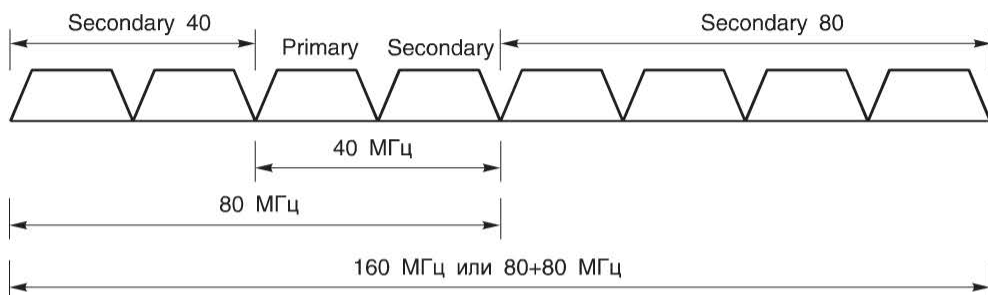


Рис. 5.57. Связь между первичными и вторичными каналами

Спецификация 802.11ac так же, как и спецификация 802.11n, не позволяет частичного перекрытия каналов 20 МГц, поскольку это приводит к значительной интерференции сигналов и усложнению методов организации сосуществования. В спецификации 802.11ac существует несколько методов выбора каналов. Прежде чем начать использовать канал, беспроводная станция должна выполнить сканирование всех каналов, чтобы найти все соседние сети. Если точка доступа начинает работать на канале шириной 20 МГц, то этот канал не должен перекрываться с вторичными каналами 20 или 40 МГц любых соседних сетей, работающих на каналах шириной 40, 80, 160 или 80+80 МГц. Если точка доступа, использующая канал шириной 40, 80, 160 или 80+80 МГц, определяет, что существуют сети, первичные каналы 20 МГц которых перекрываются с ее вторичным каналом 20 МГц, то она должна переключиться на работу в канале шириной 20 МГц и/или изменить номер канала. При выборе первичного канала точка доступа, работающая на канале шириной 40, 80, 160 или 80+80 МГц, должна убедиться, что он не перекрывается с вторичным каналом 20 МГц соседних сетей с каналами 40, 80, 160 или 80+80 МГц и/или вторичным каналом 40 МГц сетей с каналами 160 или 80+80 МГц. Если окажется, что точка доступа занимает несколько или все каналы любых соседних сетей, то она должна выбрать первичный канал так, чтобы он совпадал с первичным каналом любой из соседних сетей. Если точка доступа переходит на использование другого набора каналов или изменяется ширина используемого канала, она сообщает об этом ассоциированным с ней клиентам.

Кадр физического уровня VHT

На физическом уровне HT определено три формата кадров PLCP, которые может использовать оборудование 802.11n. По сравнению с 802.11n физический уровень 802.11ac проще и определяет только один формат кадра (рис. 5.58). Этот формат имеет преамбулу, состоящую из двух частей: преамбулы физического уровня OFDM и преамбулы физического уровня VHT, что позволяет устройствам 802.11ac работать в смешанном режиме и обеспечивать совместимость с устройствами 802.11a и 802.11n.

Преамбула 802.11ac включает ряд *обучающих полей (training field)*. Первая часть преамбулы (преамбула OFDM PHY) включает поля L-STF (Non-HT

Short Training Field), L-LTF (Non-HT Long Training Field) и L-SIG (Non-HT Signal Field). Поля L-STF и L-LTF позволяют приемнику определить начало передачи сигнала и синхронизировать таймеры. Поле L-SIG несет информацию о длине кадра в байтах и используется приемником для вычисления длительности передачи.



Рис. 5.58. Формат кадра физического уровня VHT

Следующая часть преамбулы — это преамбула физического уровня VHT. Она состоит из полей VHT-SIG-A, VHT-STF, VHT-LTF и VHT-SIG-B. Поля VHT-SIG-A (VHT Signal A) и VHT-SIG-B (VHT Signal B) понятны только устройствам 802.11ac. Вместе эти два поля используются для описания атрибутов кадра, таких как длина кадра, ширина канала, количество пространственных потоков, распределение пространственных потоков при MU-MIMO, модуляция и кодирование, и другой информации, используемой при демодуляции кадра. Поле VHT-STF (*VHT Short Training Field*) позволяет приемнику настроиться на прием сигнала. Количество полей VHT-LTF (*VHT Long Training Field*) в кадре равно количеству пространственных потоков. Эти поля позволяют приемнику вычислить многолучевые характеристики канала и применить к ним алгоритм MIMO. Также они используются функцией Beamforming в процессе оценки канала.

Модуляция и схемы кодирования

Так же, как и в спецификации 802.11n, скорость передачи в 802.11ac зависит от количества пространственных потоков, ширины канала, используемых схем модуляции и сверточного кодирования, длительности защитного интервала. Однако в отличие от 802.11n, где существует 77 возможных комбинаций этих параметров, в 802.11ac определено только 10 комбинаций, обязательными из которых являются с 0 по 7 (табл. 5.10). Еще одним упрощением в 802.11ac является использование всеми потоками, предназначенными одному пользователю, равной модуляции (*Equal Modulation*).

Таблица 5.10. Значения MCS в 802.11ac

Номер схемы MCS	Модуляция	Скорость кодирования
0	BPSK	1/2
1	QPSK	1/2
2	QPSK	3/4
3	16-QAM	1/2
4	16-QAM	3/4

Номер схемы MCS	Модуляция	Скорость кодирования
5	64-QAM	2/3
6	64-QAM	3/4
7	64-QAM	5/6
8	256-QAM	3/4
9	256-QAM	5/6

Физический уровень 802.11ac включает обязательную поддержку модуляции BPSK, QPSK, 16-QAM, 64-QAM и дополнительную поддержку модуляции 256-QAM. На рис. 5.59 показано сигнальное созвездие 256-QAM, вычисленное для реального сигнала.

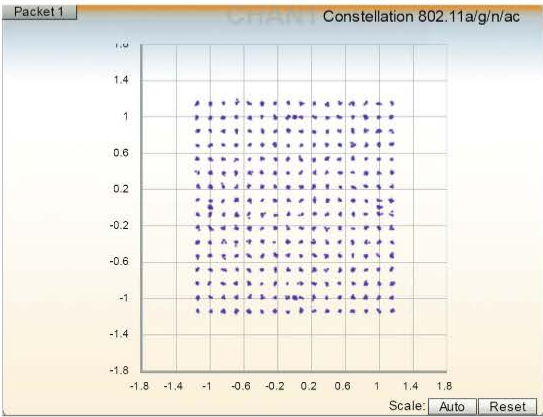


Рис. 5.59. Сигнальное созвездие модуляции 256-QAM

Для борьбы с ошибками в передаваемых кадрах в 802.11ac используются две схемы прямого исправления ошибок (FEC), аналогичные 802.11n: двоичное сверточное кодирование (*Binary Convolutional Coding, BCC*) является основным, коды LDPC (*Low-Density Parity Check*) — опциональными. Скорости кодирования в 802.11ac аналогичны скоростям кодирования в 802.11n: 1/2, 2/3, 3/4 и 5/6. Защитный интервал также не изменился: обязательный длинный защитный интервал равен 800 нс, опциональный укороченный защитный интервал — 400 нс.

Полный список скоростей физического уровня 802.11ac достаточно объемный, поэтому в табл. 5.11 приведены только некоторые из них.

Как видно из таблицы, для некоторых схем MCS вместо значения скорости стоит прочерк. Это связано с тем, что в спецификации 802.11ac несколько схем MCS обозначены как «not valid» (недействительные). Правило определения действительности схемы MCS следующее: количество закодирован-

Таблица 5.11.1. Скорости передачи в 802.11ac

Скорости передачи, Мбит/с, при укороченном GI и количестве пространственных потоков 1,2,3,8													
Но- мер схемы MCS	Модуляция и скорость кодирования	20 МГц, 1 x SS	20 МГц, 2 x SS	20 МГц, 3 x SS	20 МГц, 8 x SS	40 МГц, 1 x SS	40 МГц, 2 x SS	40 МГц, 3 x SS	40 МГц, 8 x SS	80 МГц, 1 x SS	80 МГц, 2 x SS	80 МГц, 3 x SS	80 МГц, 8 x SS
0	BPSK, 1/2	7.2	14.4	21.7	57.8	15.0	30.0	45.0	120.0	32.5	65.0	97.5	260.0
1	QPSK, 1/2	14.4	28.9	43.3	115.6	30.0	60.0	90.0	240.0	65.0	130.0	195.0	520.0
2	QPSK, 3/4	21.7	43.3	65.0	173.3	45.0	90.0	135.0	360.0	97.5	195.0	292.5	780.0
3	16-QAM, 1/2	28.9	57.8	86.7	231.1	60.0	120.0	180.0	480.0	130.0	260.0	390.0	1040.0
4	16-QAM, 3/4	43.3	86.7	130.0	346.7	90.0	180.0	270.0	720.0	195.0	390.0	585.0	1560.0
5	64-QAM, 2/3	57.8	115.6	173.3	462.2	120.0	240.0	360.0	960.0	260.0	520.0	780.0	2080.0
6	64-QAM, 3/4	65.0	130.0	195.0	520.0	135.0	270.0	405.0	1080.0	292.5	585.0	—	2340.0
7	64-QAM, 5/6	72.2	144.4	216.7	577.8	150.0	300.0	450.0	1200.0	325.0	650.0	975.0	2600.0
8	256-QAM, 3/4	86.7	173.3	260.0	693.3	180.0	360.0	540.0	1440.0	390.0	780.0	1170.0	3120.0
9	256-QAM, 5/6	—	—	288.9	—	200.0	400.0	600.0	1600.0	433.3	866.7	1300.0	3466.7

ных битов, приходящихся на один кодированный поток, должно быть целым числом. Модуляция определяет количество кодовых битов, приходящихся на одну поднесущую. Например, при модуляции 256-QAM в канале 20 МГц на одну поднесущую приходится 416 кодовых бит. При скорости кодирования $3/4$, как в MCS 8, 416 кодовых бит делятся на 104 блока. При скорости кодирования $5/6$, как в MCS 9, 416 кодовых бит не могут делиться на целое число блоков ($416/6 = 69,3$).

Расширение MIMO

Технология MIMO начала использоваться в беспроводных сетях, начиная со спецификации 802.11n. Напомним, что MIMO является радиоантенной технологией, в которой для передачи и приема используется множество антенн. В основе технологии MIMO лежит пространственное мультиплексирование. В 802.11n поддерживается передача до четырех пространственных потоков, которые одновременно и независимо друг от друга передаются через множество антенн только *одному* устройству. Такая форма MIMO называется *однопользовательской* (*Single-User MIMO*, *SU-MIMO*). К однопользовательской форме MIMO в 802.11ac добавлена *многопользовательская* форма MIMO (*Multi-User MIMO*, *MU-MIMO*) и количество передаваемых пространственных потоков увеличено до восьми (рис. 5.60).

MU-MIMO (*Multi-User MIMO*) — это технология, которая позволяет множеству станций с одной или несколькими антеннами одновременно передавать одной станции или получать от нее независимые потоки данных в одном частотном диапазоне.

Технология MU-MIMO может быть реализована несколькими способами. Наиболее часто используемые — разделение с помощью мультиплексирования с ортогональным частотным разделением (OFDMA) и разделение по пространственным потокам посредством MIMO. Метод OFDMA подразумевает, что разные поднесущие OFDM-сигнала отдаются разным пользователям. При этом при установлении соединения станция оповещает клиентов о назначенных им поднесущих во избежание коллизий. Такая многопользовательская технология эффективна при большом числе поднесущих и применяется в настоящее время в системах WiMAX 802.16.

Технология разделения пользователей по пространственным потокам реализуется в спецификации 802.11ac посредством MIMO. При этом устройство, осуществляющее многопользовательскую передачу, должно постоянно оценивать состояние радиоканала, выбирая оптимальные каналы связи для каждого приемного устройства. На рис. 5.61 показана схема передатчика 802.11ac, реализующая технологию MU-MIMO с использованием корректирующих кодов BCC и LDPC. Блок пространственного преобразования (*Spatial Mapping*) выполняет привязку пространственно-временных потоков к трактам передачи. Данное преобразование выполняется на основе анализа пространственных каналов передачи данных. Сформированный сигнал для конкретного устройства привязывается к тому тракту передачи (определенным антеннам), на котором обеспечивается наилучшая связь с данным устройством.

В 802.11ac поддерживается конфигурация *downlink MU-MIMO* (DL-MU-MIMO, нисходящая многопользовательская форма MIMO): точка доступа, имеющая множество антенн, одновременно передает независимые потоки данных множеству клиентских устройств, находящихся в одном частотном диапазоне, а клиентские устройства одновременно получают один или несколько пространственно-временных потоков от этой точки доступа. Клиентские устройства при этом не могут одновременно передавать данные точке доступа, а делают это последовательно друг за другом.

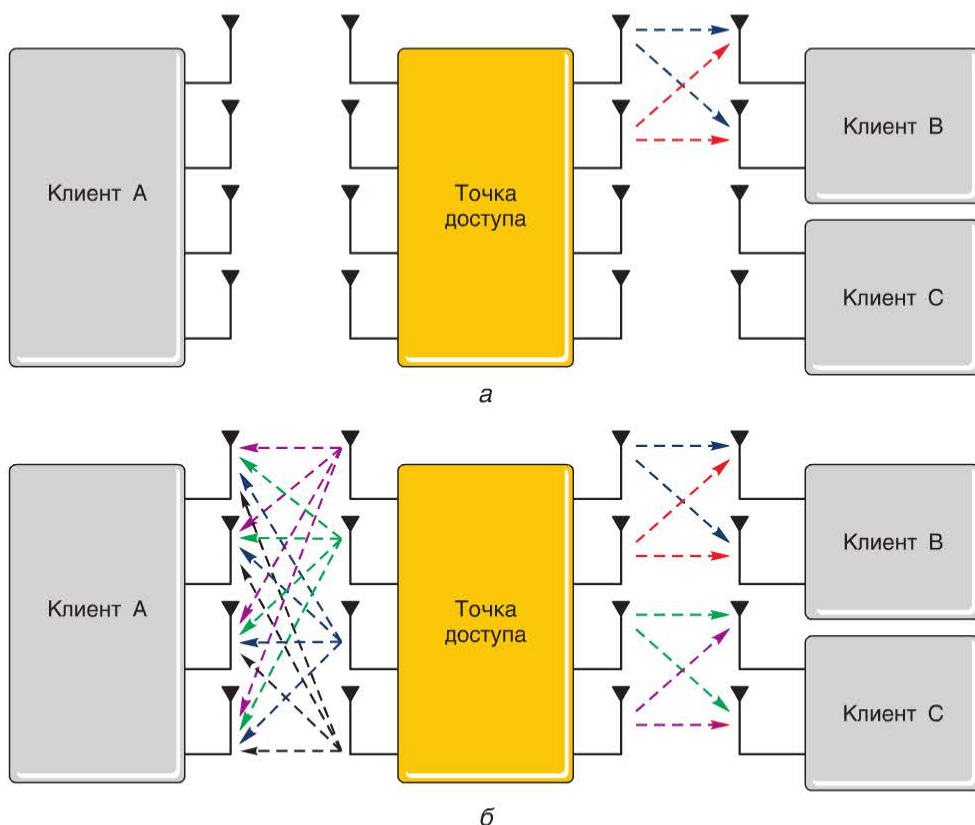


Рис. 5.60. Сравнение форм MIMO:
а — SU-MIMO; б — MU-MIMO

При использовании DL-MU-MIMO существуют следующие ограничения:

- поддерживается максимум четыре клиентских устройства;
- каждому клиентскому устройству может передаваться не более четырех пространственных потоков;
- суммарное количество пространственных потоков, одновременно передаваемых точкой доступа, не может превышать восьми.

Используя DL-MU-MIMO, точка доступа должна постоянно получать информацию о состоянии каналов до клиентов, что позволяет уменьшить

межпользовательскую интерференцию в результате одновременной передачи множества потоков. Поэтому для реализации DL-MU-MIMO спецификация 802.11ac использует метод точной оценки функции формирования диаграммы направленности, получивший название MU-Beamforming. Это позволяет точке доступа вычислять управляющие матрицы и наиболее точно направлять излучаемую энергию в сторону клиентов.

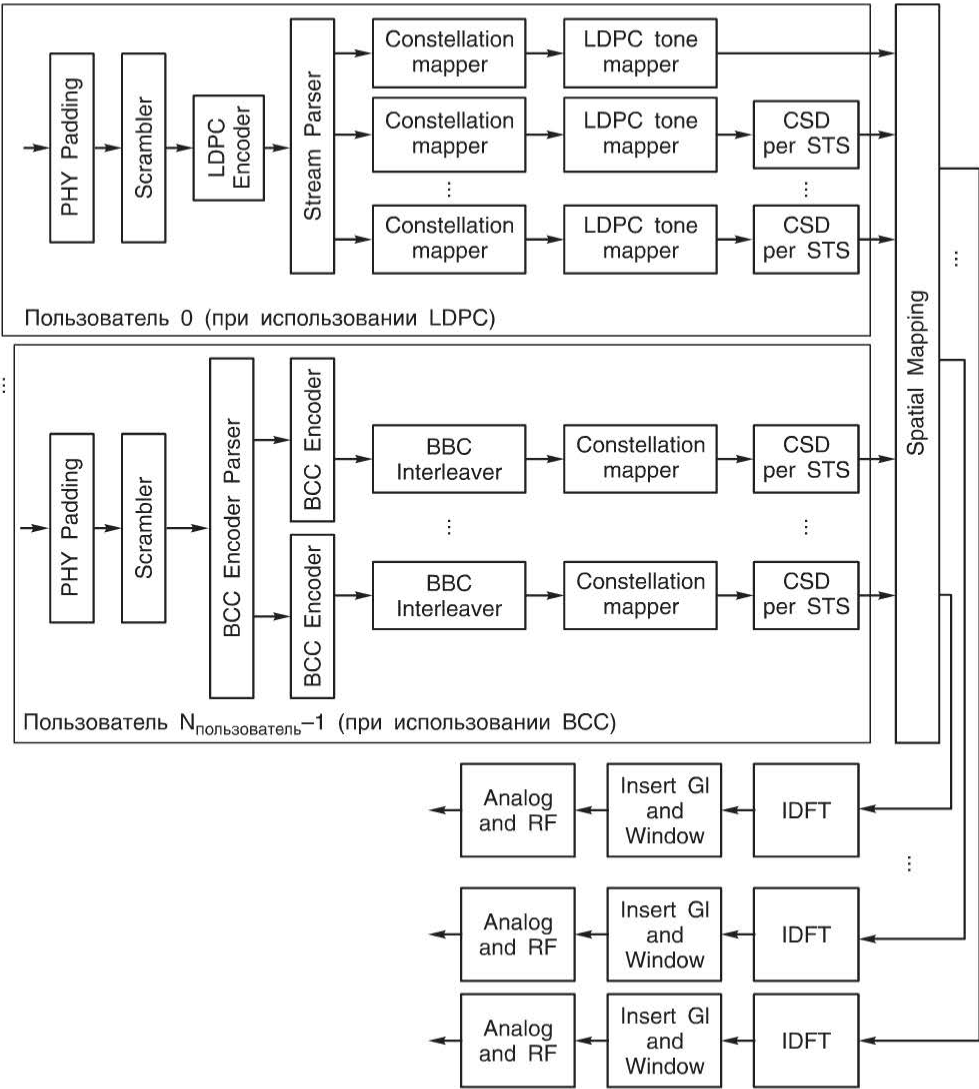


Рис. 5.61. Схема передатчика 802.11ac для реализации MU-MIMO

Конфигурация uplink MU-MIMO (UL-MU-MIMO, восходящая многопользовательская форма MIMO) в спецификации 802.11ac не поддерживается в связи со сложностью ее реализации.

Формирование диаграммы направленности передатчика

В спецификации 802.11ac для обеих форм MIMO (SU- и MU-MIMO) определен только один вариант реализации функции Beamforming, основанный на точной оценке (*explicit beamforming*). Как уже было сказано ранее, это сделано для обеспечения совместимости устройств разных производителей. Функция формирования диаграммы направленности SU-MIMO позволяет фокусировать энергию в сторону одного клиента. Функция формирования диаграммы направленности MU-MIMO позволяет фокусировать энергию в направлении нескольких клиентов.

В основе функции Beamforming спецификации 802.11ac, как и 802.11n, лежит использование «изучающих» кадров (*sounding frame*). Процесс обмена этими кадрами позволяет передатчику (формирователю луча) получать информацию о состоянии канала до разных клиентов (получателей луча). Для этого передатчик отправляет приемникам длинные обучающие символы и ожидает от них сжатые управляющие матрицы, вычисленные на основе изучения полученных обучающих символов. Управляющие матрицы вычисляются каждый раз при получении новых измерений параметров канала. Так как в случае MU-MIMO формирование лучей происходит одновременно для нескольких клиентов, то используется специальный протокол, который обеспечивает их упорядоченный опрос.

Протокол изучения параметров канала (*Sounding protocol*), предложенный для 802.11ac, работает следующим образом. Сначала формирователь луча (beamformer) передает кадр уведомления VHT NDP (*Null Data Packet Announcement*), который содержит адрес передатчика (точки доступа), адреса (или адрес в случае SU-MIMO) предполагаемых получателей (beamformee) и порядковый номер, идентифицирующий этот кадр уведомления. Целью отправления этого кадра является уведомление требуемых приемных станций о том, что они должны быть готовы к формированию кадра с управляющей матрицей.

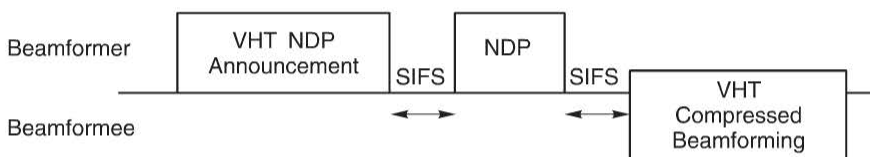


Рис. 5.62. Работа протокола Sounding в конфигурации SU-MIMO

После интервала SIFS точка доступа отправляет «изучающий» кадр VHT NDP (*Null Data Packet*). На основе полученного кадра VHT NDP приемная станция измеряет параметры канала и вычисляет сжатую управляющую матрицу, которую затем включает в свой отчет VHT Compressed Beamforming точке доступа. Кадр VHT NDP имеет такой же формат, как и кадр VHT, но при этом в нем отсутствует поле данных, поэтому получатели для измерения параметров канала между ними и точкой доступа используют только преамбулу кадра.

Первая (или единственная в случае SU-MIMO) станция-получатель отправляет точке доступа кадр VHT Compressed Beamforming через интервал SIFS после получения кадра VHT NDP (рис. 5.62).

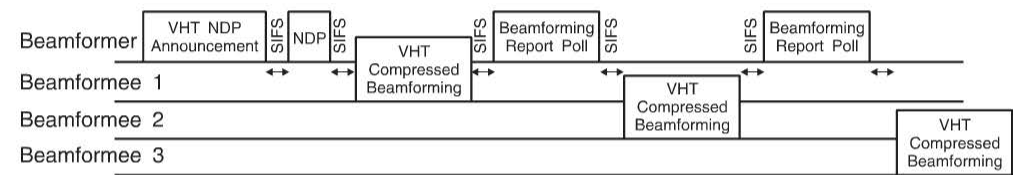


Рис. 5.63. Работа протокола Sounding в конфигурации MU-MIMO

Если кадр уведомления VHT NDPA содержит множество предполагаемых получателей, остальные станции ожидают, когда они будут опрошены точкой доступа с помощью кадра опроса Beamforming Report Poll с целью получения сжатых управляющих матриц (рис. 5.63).

5.7.2. Технологии повышения производительности на MAC-подуровне 802.11ac

Спецификация 802.11ac использует общий для всех спецификаций формат кадр MAC, но с небольшими изменениями: максимальный размер поля «Тело кадра» увеличен до 11454 байт, поле «Управление высокой пропускной способностью» имеет два варианта: HT и VHT.

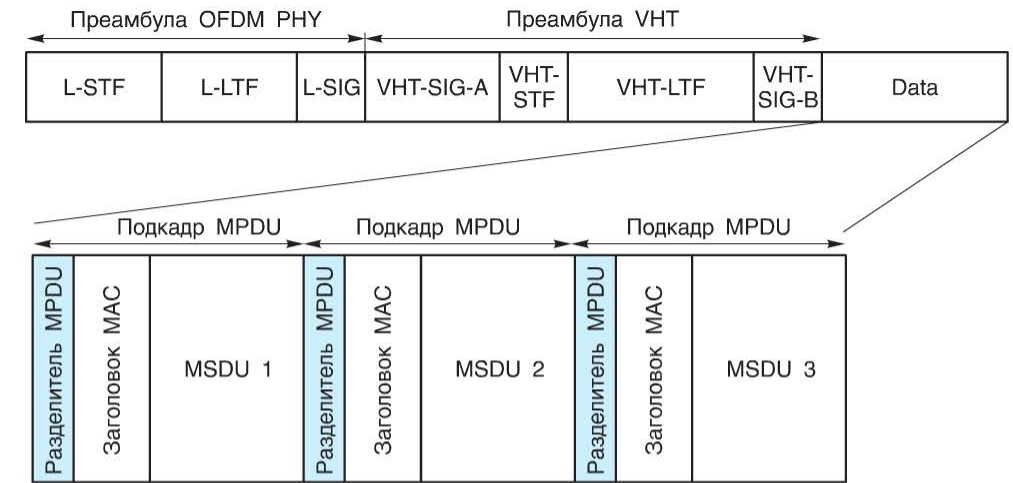


Рис. 5.64. Формат A-MPDU

Также небольшие изменения выполнены в механизмах агрегации A-MSDU и A-MPDU, определенных в 802.11n. Кадры MSDU, размер которых меньше 1500 байт, обычно агрегируются в кадр A-MSDU. Максимальный размер кадра A-MSDU в спецификации 802.11ac увеличен с 7935 байт до 11454 байт. Кадры A-MSDU инкапсулируются в MPDU. Кадры MPDU аг-

регируются в A-MPDU. Максимальный размер кадра A-MPDU в спецификации 802.11ac увеличен с 65535 байт до 1048575 байт. Другим отличием от 802.11n, помимо увеличения размера агрегированных кадров, является то, что все кадры 802.11ac передаются в формате A-MPDU (рис. 5.64). Даже если передается только один кадр MPDU, он все равно передается в формате агрегированного MPDU. Это связано с тем, что для описания высоких скоростей передачи, которые определены в 802.11ac, требуется большее количество битов. Для того чтобы не увеличивать длину преамбулы кадра физического уровня 802.11ac в поле VHT-SIG-B длина кадра указывается не в байтах, как в преамбулах кадров физического уровня 802.11a/n, а в символах OFDM. Поскольку разделитель MPDU (MPDU delimiter) кадра A-MPDU содержит информацию о длине кадра в байтах, то 802.11ac требует, чтобы каждый кадр передавался в формате A-MPDU, обеспечивая, таким образом, информацию о длине кадра в байтах.

Существенные изменения внесены в MAC-подуровень 802.11ac для обеспечения сосуществования устройств 802.11a/n/ac в одном частотном диапазоне и доступа к среде передачи с широкими каналами.

5.7.3. Механизмы защиты и сосуществования при работе в сети с устройствами 802.11a/n

Поскольку спецификация 802.11ac включает новые методы организации высокоскоростной передачи данных, кадры, передаваемые устройствами 802.11ac, «непонятны» оборудованию 802.11a/n, работающему в диапазоне 5 ГГц. В спецификации 802.11ac существует несколько механизмов организации сосуществования, основным из которых является механизм, расширяющий подход, определенный в 802.11n: использование преамбулы кадра физического уровня, состоящей из двух частей.



Рис. 5.65. Режимы работы оборудования 802.11ac D-Link

Наличие преамбулы OFDM в кадре физического уровня 802.11ac позволяет устройствам 802.11a/n определить начало передачи, вычислить ее длительность с помощью поля L-SIG и установить свои векторы NAV. Таким образом, устройства 802.11a/n могут избежать передачи кадров одновременно с устройствами 802.11ac.

В спецификации 802.11n был определен формат HT-greenfield, поддерживающий работу только с оборудованием 802.11n. Однако в реальных сетях используется в основном смешанный режим, обеспечивающий совместимость с устройствами предыдущих спецификаций. Поэтому в спецификации 802.11ac формат «greenfield» не был определен. С целью обеспечения гибкости настроек в программном обеспечении оборудования 802.11ac D-Link реализована поддержка режимов «802.11ac only», «Mixed 802.11ac and 802.11n» и «Mixed 802.11ac, 802.11n and 802.11a» (рис. 5.65).

Защита и динамическое выделение каналов

В диапазоне 5 ГГц существует достаточное количество каналов шириной 20 и 40 МГц и во избежание полного или частичного перекрытия между соседними сетями можно просто выбрать различные каналы. При использовании каналов 80 и 160 МГц это становится сделать труднее. Также сложнее становится выбрать общий для всех перекрывающихся сетей первичный канал.

В случае когда точка доступа 802.11ac работает на канале шириной 80 или 160 МГц, а первичные каналы 20 МГц соседних сетей 802.11a/n перекрываются с любым из подканалов внутри этого широкого канала, возникает проблема избежания одновременной передачи с соседними станциями.

Для решения этой проблемы, надо ответить на три вопроса.

- Как станция (точка доступа или клиент), которая хочет начать работу на канале шириной 80 или 160 МГц, предупредит станции 802.11a/n, чтобы они прекратили передачу на время, требуемое для передачи кадров в режиме 802.11ac?

- Как станция 802.11ac узнает, что канал 80 или 160 МГц полностью свободен от передач других устройств?

- Как можно оптимизировать использование полосы пропускания, если, например, устройства 802.11a/n занимают для передачи только полосу шириной 20 МГц канала 80 МГц?

Чтобы решить эти проблемы, в спецификации 802.11ac расширены возможности функции *clear channel assessment* (CCA) во вторичном канале и появился механизм работы с динамической полосой пропускания.

Для того чтобы уведомить станции стандартов 802.11a/n о начале передачи, станция 802.11ac использует расширенный механизм RTS/CTS. Напомним, что первоначальный стандарт 802.11 определил механизм RTS/CTS для решения проблемы скрытых узлов. Впоследствии кадры CTS стали использоваться для управления доступом к среде передачи при наличии в сети устройств устаревших стандартов. Кадры RTS и CTS используются только для управления доступом к сети. Их можно передавать на низких скоростях, поэтому они будут получены и поняты всеми станциями сети.

В 802.11ac механизм RTS/CTS модифицирован таким образом, что он предоставляет информацию о *доступной полосе пропускания (bandwidth signaling)*. Рассмотрим пример обмена кадрами RTS/CTS. Предположим, что станция 802.11ac хочет передать кадр данных и использовать для передачи канал шириной 80 МГц. Сначала она проверяет свободен ли канал, выполняя функцию *clear channel assessment (CCA)*. Далее, если среда свободна, станция параллельно отправляет одинаковые кадры RTS в формате 802.11a PPDU в каждый из 20-мегагерцевых подканалов канала 80 МГц. В зависимости от ширины канала 802.11ac может одновременно передаваться два (40 МГц), четыре (80 МГц) или восемь (160 МГц) кадров RTS. Отправляя множество кадров RTS, станция ожидает, что каждое соседнее устройство (802.11a/n или 802.11ac) сможет получить кадр RTS в своем первичном канале. Для того чтобы сделать протокол более надежным, в кадре RTS отправитель указывает ширину своего канала (20, 40, 80, 160 или 80+80 МГц). Для этого в кадре RTS первый бит MAC-адреса передатчика изменяется с индивидуального на групповой, а скремблированная последовательность кадра физического уровня 802.11a, в который помещается RTS, кодирует ширину канала.

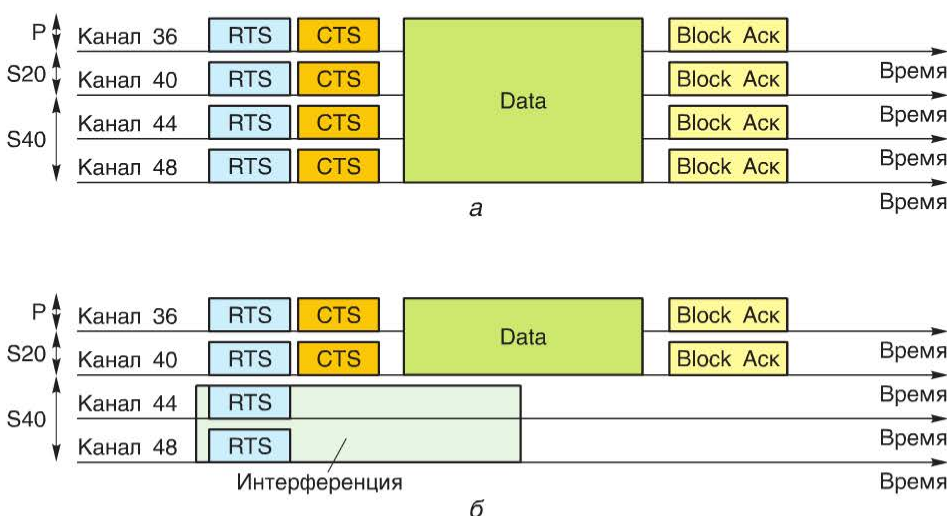


Рис. 5.66. Расширенный механизм RTS/CTS при отсутствии интерференции (а) и при интерференции (б)

Прежде чем ответить кадром CTS, каждый получатель в течение интервала PIFS прослушивает среду (выполняет функцию CCA) во всех вторичных каналах того канала, ширина которого указана в кадре RTS, в нашем примере — внутри канала шириной 80 МГц. Изменения, сделанные в спецификации 802.11ac, позволяют функции CCA лучше определять наличие соседних сетей во вторичных каналах по сравнению со спецификацией 802.11n.

Получатель отвечает кадром CTS только в свободных подканалах. В кадре ответа он сообщает отправителю общую полосу пропускания свободных

каналов (доступную ширину канала). Аналогично кадрам RTS кадры CTS отправляются в формате физического уровня 802.11a и дублируются во всех свободных подканалах 20 МГц.

Если все подканалы 20 МГц оказались свободными, станция 802.11ac отправляет кадр данных, используя всю полосу пропускания канала 80 МГц (рис. 5.66, а). Если какие-то подканалы оказались заняты, станция 802.11ac передает данные только через доступную для использования часть канала 80 МГц (рис. 5.66, б). Получатель отправляет кадр блочного подтверждения Block Ack, продублированный во всех свободных подканалах.

Занятость подканалов приводит к тому, что полоса пропускания может сократиться до 40 или 20 МГц. Однако несмотря на это, станция 802.11ac все равно имеет возможность передать данные пусть и на уменьшенной полосе пропускания. Эта функция станций 802.11ac называется *работа с динамической полосой пропускания (dynamic bandwidth operation)*. Альтернативным вариантом является *работа со статической полосой пропускания (static bandwidth operation)*. В этом случае получатель отвечает кадром CTS только в том случае, если весь канал свободен. Если хоть один из подканалов занят, получатель не отправляет кадр CTS, и отправитель должен снова начать процедуру доступа к каналу. Отправитель сможет передать кадр только в том случае, если все подканалы окажутся свободными.

5.7.4. Downlink Multi-User MIMO

Одним из методов повышения производительности в сетях 802.11ac является использование многопользовательской формы MIMO (MU-MIMO). В ее основе, как и в однопользовательской форме MIMO, лежит пространственное мультиплексирование (*spatial multiplexing*), при котором множество независимых потоков данных одновременно передаются через множество антенн. В отличие от однопользовательской формы MIMO, при которой все потоки передаются только одному устройству, многопользовательская форма позволяет одновременно и независимо передавать потоки данных нескольким устройствам. В 802.11ac поддерживается конфигурация *downlink MU-MIMO (DL-MU-MIMO)*. В этой конфигурации точка доступа, имеющая множество антенн, может одновременно передавать независимые потоки данных множеству клиентских устройств, которые передают данные точке доступа последовательно друг за другом. Рассмотрим пример домашней сети, показанной на рис. 5.67. Предположим, имеется точка доступа 802.11ac с шестью антеннами, смартфон с одной антенной (STA1), компьютер с установленным сетевым адаптером с двумя антеннами (STA2) и приставка к телевизору, имеющая две антенны (STA3). В такой ситуации точка доступа может одновременно передавать один поток данных смартфону, два потока данных компьютеру и два потока данных телевизионной приставке.

Основным преимуществом DL-MU-MIMO является то, что устройства с ограниченными возможностями (например, с одной антенной) не влияют на производительность сети, слишком долго занимая среду из-за своих низких

скоростей передачи. В конфигурации DL-MU-MIMO выполняется агрегация клиентов для одновременной передачи им данных. При этом преимущества DL-MU-MIMO ведут к повышению сложности и стоимости устройств.

С точки зрения физического уровня антенн у точки доступа должно быть больше, чем общее количество пространственных потоков. Помимо этого точка доступа должна получать информацию о состоянии канала от каждого клиента, участвующего в передаче DL-MU-MIMO, поскольку полоса пропускания DL-MU-MIMO очень чувствительна к межпользовательской интерференции в результате одновременной передачи множества потоков. Для реализации DL-MU-MIMO спецификация 802.11ac использует метод точной оценки функции Beamforming, что позволяет точке доступа вычислять управляющие матрицы и наиболее точно направлять излучаемую энергию в направлении клиентов. Информация о состоянии канала должна быть точной и часто обновляемой. В противном случае, если параметры управляющей матрицы неточно соответствуют каналу, потоки, направляемые одному из устройств, будут влиять на потоки других устройств, что приводит к интерференции.

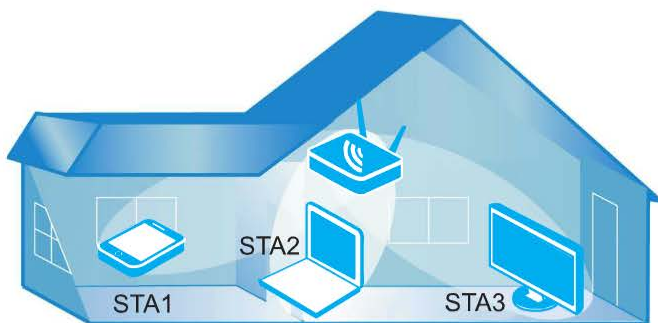


Рис. 5.67. Пример DL-MU-MIMO

Чтобы ограничить размер системы, в спецификации 802.11ac зафиксировано максимальное количество клиентов в конфигурации DL-MU-MIMO, равное 4, максимальное количество пространственных потоков, передаваемых одному пользователю, 4, максимальное суммарное количество пространственных потоков, одновременно передаваемых всем клиентам, 8.

Напомним, что преамбула кадра физического уровня 802.11ac состоит из двух частей: преамбулы физического уровня OFDM и преамбулы физического уровня VHT. Кадр физического уровня MU-MIMO имеет точно такую же структуру преамбулы, что и кадр SU-MIMO. Однако преамбула физического уровня VHT определяется для каждого клиента в отдельности, и в поле VHT-SIG-B помещаются параметры, относящиеся к конкретному клиенту.

Для того чтобы время передачи кадра каждому клиенту было одинаковым, на MAC-подуровне может потребоваться дополнить кадры некоторым числом байтов до требуемого размера. На физическом уровне к кадру каждого клиента может добавляться несколько битов, чтобы получить одинаковое количество символов.

Клиенты узнают, что они являются частью многопользовательской передачи благодаря параметру *Group ID* (идентификатор группы) в поле VHT-SIG-A преамбулы VHT. Прежде чем начать многопользовательскую передачу, точка доступа передает информацию о группе всем клиентам в BSS, поддерживающим DL-MU-MIMO. Основываясь на Group ID, можно создать до 62 групп клиентских устройств. Дополнительно к Group ID в поле VHT-SIG-A содержится таблица, показывающая, сколько потоков данных должно передаваться каждому клиенту в данной передаче (рис. 5.68).

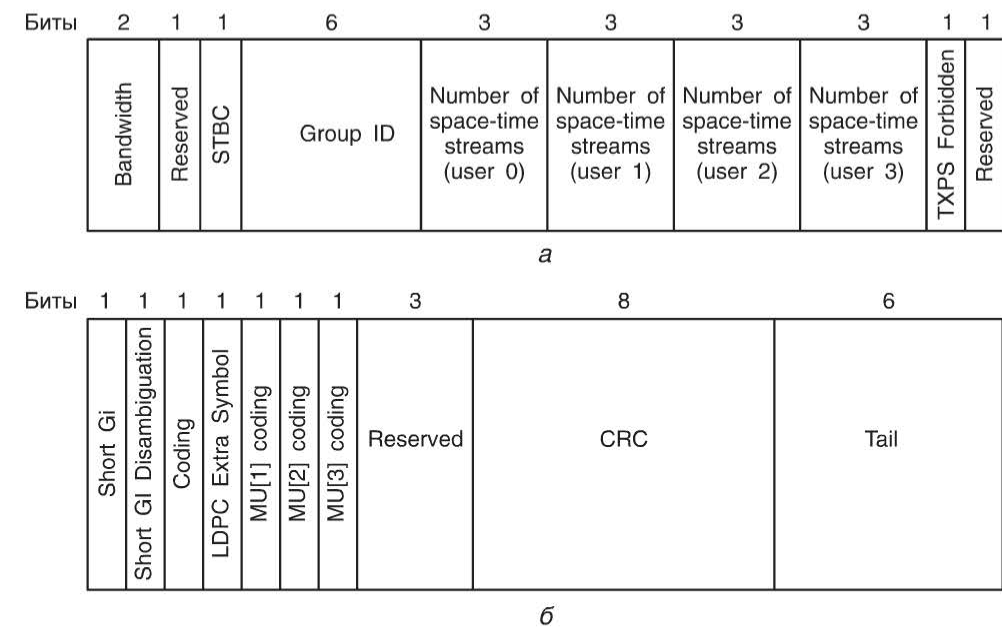


Рис. 5.68. Структура поля VHT-SIG-A: VHT-SIG-A1 (a); VHT-SIG-A2 (б)

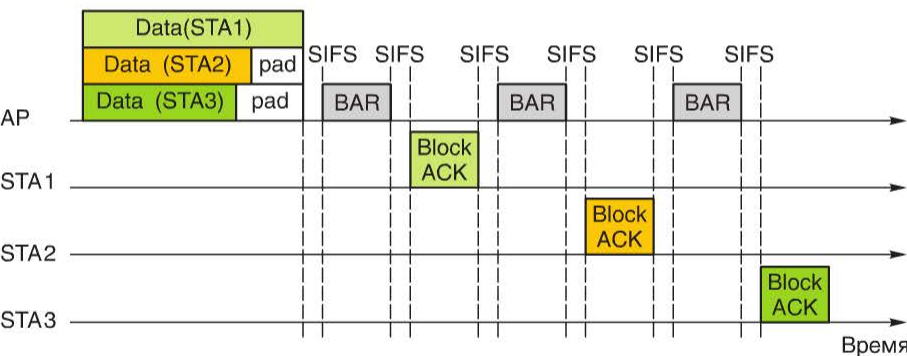


Рис. 5.69. Блочные подтверждения при многопользовательской передаче

Поскольку в конфигурации DL-MU-MIMO точка доступа одновременно передает кадры разным клиентам, необходим механизм подтверждения приема от этих клиентов. Напомним, что каждый кадр в 802.11ac передается в формате A-MPDU, что требует использования блочных подтверждений (*Block Acknowledgement*), как было изначально определено в 802.11n. Клиенты последовательно отвечают точке доступа блочными подтверждениями после получения от нее запроса на подтверждение (*Block Acknowledgement Request, BAR*) (рис. 5.69).

После определения многопользовательских групп кадры, помещенные в буфер точки доступа, должны быть сгруппированы соответствующим образом, чтобы обеспечить оптимальную пропускную способность. Системы DL-MU-MIMO поддерживают четыре независимые очереди передачи, по одной для каждой категории доступа (*Background, Best Effort, Video, Voice*), как было определено в дополнении к стандарту IEEE 802.11e. Процесс организации очередей в DL-MU-MIMO значительно сложнее, поскольку одна многопользовательская передача может содержать как высокоприоритетные, так и низкоприоритетные кадры. При этом точка доступа может начать передачу низкоприоритетных кадров раньше высокоприоритетных, если ими была получена возможность передачи (*transmission opportunity, TXOP*) (рис. 5.70).

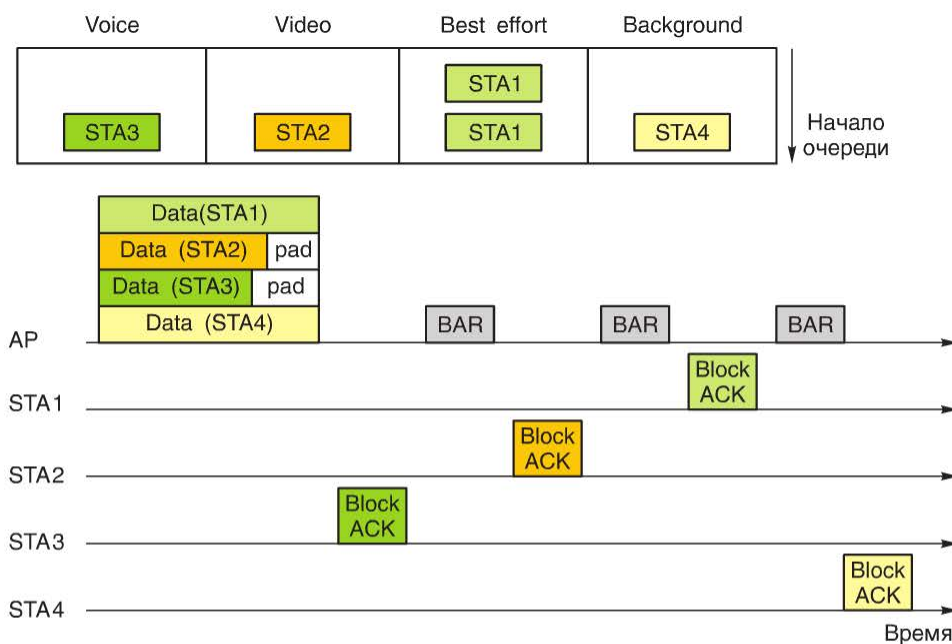


Рис. 5.70. Пример организации очередей в DL-MU-MIMO

5.7.5. Выход оборудования 802.11ac на рынок

Физические уровни спецификаций 802.11, 802.11a, 802.11b, 802.11g не поддерживают большого количества функций и достаточно просты в реализации. Поэтому устройства этих спецификаций появлялись на рынке достаточно оперативно и включали все возможности, прописанные в стандарте. Физические уровни 802.11n и 802.11ac значительно сложнее по сравнению со своими предшественниками. Реализация всех возможностей спецификации 802.11ac на практике является достаточно сложной задачей, требующей разработки и создания новых схем радиомодулей, более производительных процессоров и принципов управления ими. Поэтому добавление в оборудование спецификации 802.11ac новых функций выполняется поэтапно. Частичная реализация функций упрощает разработку новых устройств (за счет последовательного добавления новых опций) и организацию их производства. По мере расширения возможностей оборудование 802.11ac появляется на рынке в виде волн (Wave). Оборудование первой волны (Wave 1) поддерживает до трех пространственных потоков, ширину канала до 80 МГц, модуляцию 256-QAM и метод точной оценки канала функции Beamforming. Максимальная скорость передачи при использовании трех пространственных потоков – 1,3 Гбит/с. При использовании одного и двух потоков максимальные скорости соответственно 433 и 866,7 Мбит/с. Вторая волна (Wave 2) оборудования 802.11ac предполагает внедрение технологии Multi-User MIMO, поддержку более трех пространственных потоков, каналов шириной до 160 МГц, включая 80+80 МГц, и механизма работы с динамической полосой пропускания. Такие усовершенствования позволят увеличить скорости передачи до 3,467 Гбит/с. В оборудовании последующих волн будет увеличиваться количество потоков и скорость передачи.

6. Оценка беспроводной линии связи

6.1. Общие сведения

Для передачи сигналов в беспроводных сетях Wi-Fi используются волны сантиметрового диапазона SHF (*Super High Frequency* — сверхвысокие частоты, СВЧ, частоты от 3 до 30 ГГц). Эти волны распространяются преимущественно прямолинейно и почти не огибают природных и искусственных преград, встречающихся на их пути. Поэтому на распространение волн сантиметрового диапазона существенное влияние оказывают рельеф местности, различные препятствия и метеорологические условия. В частности, они сильно поглощаются и рассеиваются атмосферными явлениями (дождь, снег, туман и пр.) и газами атмосферы, что, в свою очередь, приводит к быстрому ослаблению напряженности электромагнитного поля сигналов. Учитывая это, при проектировании беспроводных линий связи приемник и передатчик обычно располагают в зоне прямой видимости друг друга.

Для любой системы связи справедливо утверждение, что принимаемый сигнал отличается от переданного вследствие различных искажений в процессе передачи. Существуют различные типы искажений, но наибольшее влияние на пропускную способность каналов связи в пределах прямой видимости оказывают рассеяние, потери в свободном пространстве за счет препятствий, шум, многолучевое распространение и атмосферное поглощение.

Проектирование беспроводных сетей практически невозможно без оценки пригодности линии связи, так как эта оценка имеет большое значение для выявления возможных проблем в ходе развертывания сети. Наличие хорошего энергетического потенциала является базовым условием для нормального функционирования линии связи.

Энергетический потенциал (Link budget) беспроводной линии связи учитывает все усиления и потери уровня сигнала при его распространении от передатчика к приемнику через беспроводную среду передачи, кабели, разъемы и различные препятствия (стены, потолки, деревья и т. д.). Оценка уровня сигнала на концах беспроводной линии связи помогает при разработке проекта сети и выборе оборудования.

Беспроводную линию связи можно разделить на три основные части: сторону передатчика, область распространения и сторону приемника (рис. 6.1). В определении энергетического потенциала беспроводной линии связи участвуют следующие параметры этих трех частей:

- эквивалентная (эффективная) изотропно-излучаемая мощность передатчика (EIRP), являющаяся суммой выходной мощности передатчика и коэффициента усиления антенны за вычетом потерь в антенном кабеле и разъемах передающего тракта;
- потери при распространении;
- чувствительность приемника, потери в антенном кабеле и коэффициент усиления антенны приемника.

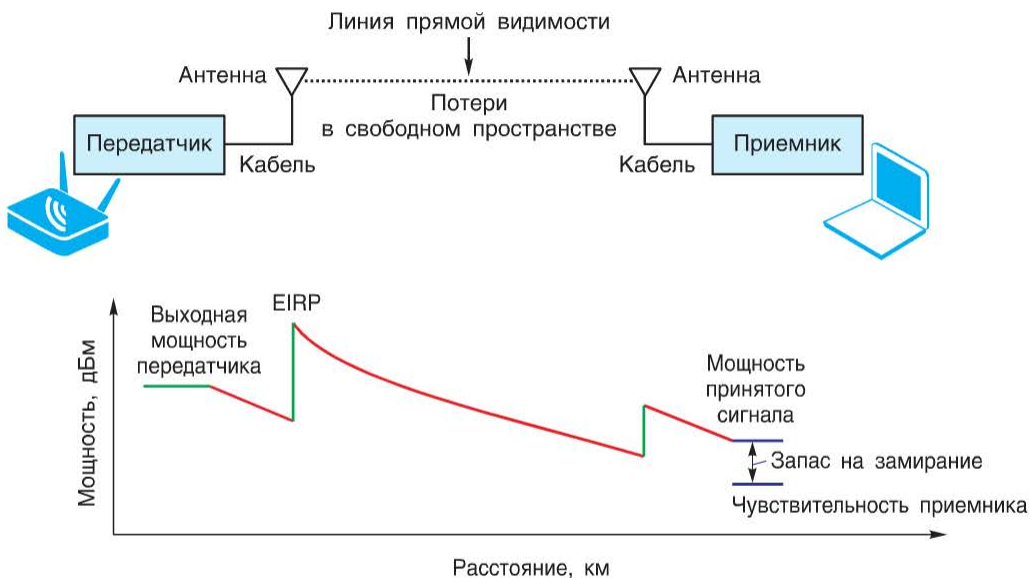


Рис. 6.1. Беспроводная линия связи

Полное уравнение энергетического потенциала линии связи можно записать следующим образом:

$$P_{tr} - L_{tr} + G_{tr} - L_{bf} + G_{rcv} - L_{rcv} = SOM + P_{rcv},$$

где P_{tr} — мощность передатчика, дБм (dBm); L_{tr} — потери сигнала в антенном кабеле и разъемах передающего тракта, дБ (dB); G_{tr} — коэффициент усиления передающей антенны, дБ (dBi); L_{bf} — потери передачи в свободном пространстве, дБ (dB); G_{rcv} — коэффициент усиления приемной антенны, дБ (dBi); L_{rcv} — потери сигнала в антенном кабеле и разъемах приемного тракта, дБ (dB); SOM — запас на замирание сигнала (SOM , *System Operating Margin*), дБ (dB); P_{rcv} — чувствительность приемника при данной скорости передачи, дБм (dBm).

Рассмотрим каждый из параметров этого уравнения.

Сторона передатчика

Выходная мощность передатчика (transmitter output power) — величина, характеризующая мощность радиосигнала, подводимого к антенне. Значение выходной мощности передатчика можно найти в техническом описании устройства. Следует обратить внимание на то, что выходная мощность указывается отдельно для каждого поддерживаемого устройством стандарта и конкретных скоростей. При этом сообщается о температуре и/или других параметрах, при которых эта мощность достигается в лабораторных условиях. В реальной сети значения мощности могут незначительно отличаться.

Таблица 6.1. Мощности передатчиков точки доступа и беспроводного адаптера

Устройство	Протокол	Мощность передатчика
DAP-2310	IEEE 802.11b	18 dBm (± 2 dB) при 1, 2, 5.5, 11 Мбит/с
	IEEE 802.11g	18 dBm (± 2 dB) при 6~24, 36, 48, 54 Мбит/с
	IEEE 802.11n	HT20: 18 dBm (± 2 dB) при MCS0-6 17 dBm (± 2 dB) при MCS7 HT40: 18 dBm (± 2 dB) при MCS0-6 17 dBm (± 2 dB) при MCS7
DWA-182	IEEE 802.11a	18 dBm при 6 Мбит/с 15 dBm при 54 Мбит/с
	IEEE 802.11b	19 dBm при 1 Мбит/с 17 dBm при 11 Мбит/с
	IEEE 802.11g	18 dBm при 6 Мбит/с 15 dBm при 54 Мбит/с
	IEEE 802.11n	2,4 ГГц/HT20: 18 dBm при MCS0-6 15 dBm при MCS7 2,4 ГГц/HT40: 18 dBm при MCS0-6 15 dBm при MCS7 5 ГГц/HT20: 18 dBm при MCS0-6 15 dBm при MCS7 5 ГГц/HT40: 18 dBm при MCS0-6 15 dBm при MCS7
	IEEE 802.11ac	18 dBm при MCS0-6 15 dBm при MCS7 13 dBm при MCS8 12 dBm при MCS9

Предельная мощность передатчика определяется государственными органами. Ее пороговое значение в оборудовании стандартов 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac не превышает 100 мВт (20 дБм). В табл. 6.1 приведены значения мощностей передатчиков точки доступа D-Link DAP-2310 и беспроводного адаптера D-Link DWA-182.

Потери мощности (затухание) сигнала могут иметь место в кабелях, с помощью которых приемник и передатчик присоединяются к антеннам.



Рис. 6.2. Кабель для антенны D-Link ANT70-CB1N длиной 1 м с разъемами N Plug

Эти потери, называемые потерями сигнала в антенном кабеле, зависят от типа кабеля и рабочей частоты. Удельные потери обычно измеряются в дБ/м (dB/m). В целом характеристики кабеля, т. е. его качество, не имеют значения, поскольку в них всегда имеет место затухание сигнала. Поэтому при подключении антенны к устройству желательно использовать максимально короткий кабель. Типичные потери

в кабеле составляют 0,1...2 дБ/м. Как уже упоминалось, потери в кабеле зависят от рабочей частоты. Поэтому при расчете линии связи требуется учитывать значения потерь для соответствующего частотного диапазона, которые обычно указаны в технических характеристиках кабеля.

Затухание сигнала увеличивают также кабельные разъемы (рис. 6.2). Величина вносимого затухания зависит от типа разъема. Для кабельной сборки, т. е. кабеля с присоединенными разъемами, потери в них уже учтены в потерях кабеля (табл. 6.2).

Таблица 6.2. Потери в кабелях D-Link

Модель	Длина, м	Диапазон частот, ГГц	Потери, дБ
ANT70-CB1N	1	2,4	0,8
		5,15–5,85	2
ANT24-ODU03M	0,3	2,4–2,5	От 0,45 до 0,6
		5,15–5,75	От 1 до 1,15
ANT24-ODU3M	3	2,4–2,5	От 0,85 до 1
		5,15–5,75	От 1,6 до 1,75

Затухание сигналов также вызывается модулем грозозащиты, который может устанавливаться между внешней антенной и беспроводным устройством для защиты последнего от высоких разрядов электрического тока во время грозы. Потери, вносимые модулем грозозащиты D-Link ANT70-SP (рис. 6.3), составляют 0,8 дБ.



Рис. 6.3. Модуль грозозащиты D-Link ANT70-SP

Типичный коэффициент усиления антенн D-Link лежит в диапазоне от 2...5 dBi (для простых встроенных и штыревых антенн) до 21 dBi (для параболических антенн). При установке антенн следует учитывать, что коэффициент усиления может оказаться ниже заявленного по ряду причин, основной из которых является неправильная уста-

новка (неверный расчет угла наклона антенны, ошибки поляризации). Коэффициент усиления также снижается под воздействием атмосферных осадков, особенно из-за обледенения или налипания снега.

Фактическая мощность сигнала, излучаемая антенной, называется *эквивалентной (эффективной) изотропно-излучаемой мощностью (ЭИИМ, англ. EIRP, Equivalent (Effective) Isotropically Radiated Power)*. Она определяется как сумма выходной мощности передатчика и коэффициента усиления антенны за вычетом потерь сигнала в кабеле и разъемах передающего тракта. Этот параметр регулируется государственными органами. ЭИИМ входит в уравнение энергетического потенциала линии связи, но в явном виде его выделять не принято.

Потери при распространении

К потерям при распространении относятся все виды затухания сигнала, которые имеют место при его распространении от антенны передатчика к антенне приемника.

Передаваемый сигнал рассеивается по мере его распространения в пространстве (в качестве аналогии можно представить падение интенсивности луча фары автомобиля с увеличением расстояния). Поэтому мощность сигнала, принимаемого антенной, будет уменьшаться по мере увеличения расстояния от передающей антенны. Данный тип затухания называют *потерями в свободном пространстве (Free Space Path Loss, FSPL)*. Они приводят к ослаблению сигнала при его прохождении от передатчика до приемника, даже если все остальные причины затухания отсутствуют. Потери линии связи с изотропными антеннами в свободном пространстве можно рассчитать с помощью следующей формулы:

$$L_{bf} = 20\lg F + 20\lg D + K,$$

где L_{bf} — потери линии связи в свободном пространстве, дБ; F — центральная частота канала, на котором работает система связи; D — расстояние между двумя антеннами; K — константа, которая зависит от единиц измерения частоты и расстояния и может меняться в зависимости от того, в каких единицах выражены частота и расстояние:

- для частоты, выраженной в ГГц, и расстояния, измеряемого в километрах, константа равна 92,45;
- для частоты, выраженной в МГц, и расстояния, измеряемого в километрах, константа равна 32,4;
- для частоты, выраженной в МГц, и расстояния, измеряемого в метрах, константа равна -27,55.

Для неизотропных антенн следует учитывать их коэффициент усиления. В результате выражение для потерь в свободном пространстве принимает следующий вид:

$$L_{bf} = 20\lg F + 20\lg D - G_{tr} - G_{recv} + K,$$

где G_{tr} — коэффициент усиления передающей антенны; G_{recv} — коэффициент усиления приемной антенны.

В качестве примера найдем потери в свободном пространстве на линии связи между двумя устройствами 802.11n (точкой доступа и клиентом) с изотропными антеннами. Устройства работают на канале 6 (центральная частота 2437 МГц). Расстояние между ними 100 м. Затухание сигнала при этих условиях составит:

$$L_{bf} = 20 \lg(2437) + 20 \lg(100) - 27,55 = 80,2 \text{ дБ.}$$

Если используется частотный диапазон 5 ГГц, то затухание сигнала на линии связи между двумя устройствами 802.11n или 802.11ac с изотропными антеннами, работающими, например, на канале 36 (центральная частота 5180 МГц) и расстоянии 100 м друг от друга, будет следующим:

$$L_{bf} = 20 \lg(5180) + 20 \lg(100) - 27,55 = 86,7 \text{ дБ.}$$

Выполним аналогичные расчеты с теми же условиями с учетом коэффициентов усиления антенн. В большинстве случаев коэффициент усиления антенн внутриофисных точек доступа и беспроводных адаптеров составляет 2 dBi.

В диапазоне 2,4 ГГц потери в свободном пространстве

$$L_{bf} = 20 \lg(2437) + 20 \lg(100) - 27,55 - 2 - 2 = 76,2 \text{ дБ.}$$

В диапазоне 5 ГГц потери в свободном пространстве

$$L_{bf} = 20 \lg(5180) + 20 \lg(100) - 27,55 - 2 - 2 = 82,7 \text{ дБ.}$$

Внимание: при расчете потерь в свободном пространстве можно воспользоваться любым бесплатным калькулятором, доступным в Интернете.

Из уравнения для изотропной антенны видно, что увеличение частоты сигнала приводит к росту потерь в свободном пространстве, которые, в свою очередь, можно компенсировать, увеличивая коэффициент усиления антенны.

Приведенные расчеты проводились для линии связи в пределах прямой видимости. Однако в реальных сетях на пути распространения сигнала встречаются различные препятствия (например, стены, потолок, мебель), которые могут в большей или меньшей степени влиять на его затухание.

Величина затухания зависит от частоты сигнала и материала, через который он проходит. В табл. 6.3 приведены величины затухания сигналов при их распространении в различных средах.

Таблица 6.3. Затухание сигналов в различных средах

Среда распространения сигналов	Затухание, дБ
Человеческое тело	3
Окно в кирпичной стене	2
Офисное окно	3
Стекло в металлической раме	6

Среда распространения сигналов	Затухание, дБ
Стекло	3–20
Стена из гипсокартона	3
Кирпичная стена, следующая за металлической дверью	3
Мрамор	5
Стеклянная стена в металлической раме	6
Стена из шлакобетона	4
Стена из сухой кладки	4
Офисная стена	6
Кирпичная стена	2–8
Бетонная стена	10–15
Деревянная дверь	3
Железная дверь в офисной стене	7
Железная дверь в кирпичной стене	12–13
Стекловолокно	0,5–1
Дождь и туман (на км)	0,02–0,05
Деревья (на м)	0,35

Предположим, что точка доступа и клиентское устройство находятся в соседних комнатах, разделенных стеной из гипсокартона, ослабляющей сигнал на 3 дБ. Учитывая потери в свободном пространстве при рассмотренных ранее условиях, определим суммарное ослабление сигнала. В диапазоне 2,4 ГГц затухание составит 79,2 дБ (76,2 дБ + 3 дБ), а в диапазоне 5 ГГц оно будет равно 85,7 дБ (82,7 дБ + 3 дБ) (рис. 6.4).

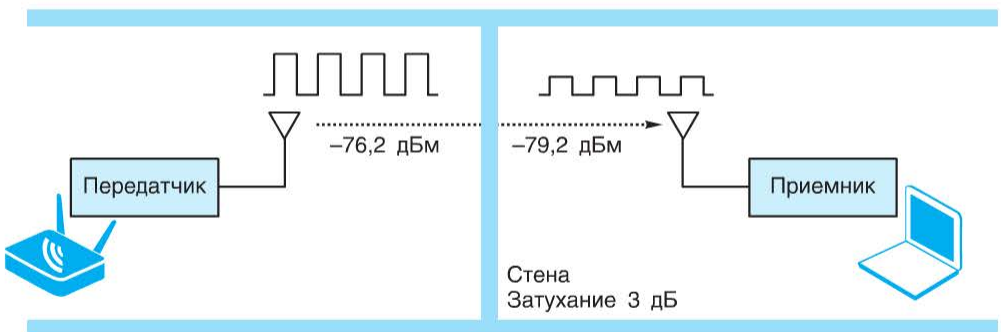


Рис. 6.4. Влияние препятствия (стены из гипсокартона) на затухание сигнала

При развертывании уличных беспроводных сетей следует учитывать, что причиной дополнительных потерь мощности сигнала является атмосферное поглощение, при этом основной вклад в ослабление сигнала вносят водяные пары и кислород. Дождь и туман (капли воды, находящиеся во взвешенном состоянии в воздухе) приводят к рассеянию радиоволн и в конечном счете к ослаблению сигнала. Следует отметить, что при расчете затухания сигнала в осадках (дождь, туман, снег) величина затухания будет зависеть также и от интенсивности осадков.

Как упоминалось ранее, для эффективной связи с помощью сантиметровых волн требуется обеспечить беспрепятственную линию прямой видимости между передатчиком и приемником, что не всегда возможно. Для определения того, сколько свободного от преград пространства должно быть на линии связи, между передатчиком и приемником используется такое понятие, как *зона Френеля (Fresnel Zone)*.

Понятие зон Френеля основано на принципе Гюйгенса. В соответствии с моделью Френеля область распространения радиоволн между передающим и приемным устройствами ограничивается эллипсоидом вращения вокруг соединяющей их линии. Эллипсоид многослойный и может включать в себя бесконечное число зон. На основе принципа Гюйгенса можно показать, что объекты, лежащие внутри эллипсоидов вращения, могут влиять на качество связи.

Ближайшая зона к линии, соединяющей передатчик с приемником, называется первой зоной Френеля (рис. 6.5). Все естественные (земля, холмы, деревья) и искусственные (здания, столбы) препятствия, попадающие в нее, оказывают наиболее негативное влияние на уровень сигнала в результате отражения, преломления, рассеяния или дифракции. При этом чем длиннее линия связи, тем важнее становится вычисление радиуса первой зоны Френеля.

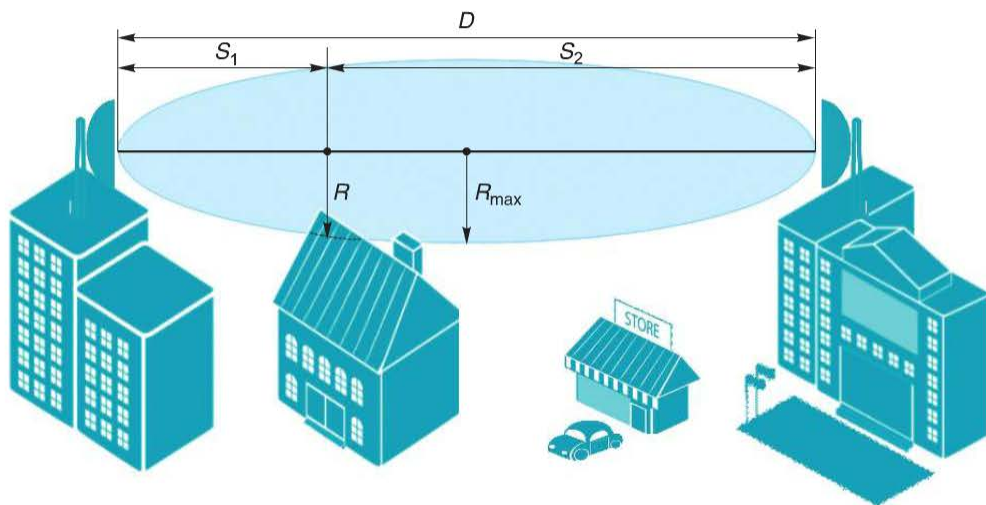


Рис. 6.5. Первая зона Френеля

Для любой точки радиолинии радиус первой зоны Френеля можно найти по формуле

$$R = 17,32 \sqrt{\frac{S_1 S_2}{F(S_1 + S_2)}},$$

где R — радиус первой зоны Френеля, м; S_1 — расстояние от антенны передатчика до самой высшей точки предполагаемого препятствия, км; S_2 — расстояние от самой высшей точки предполагаемого препятствия до антенны приемника, км; F — частота, ГГц.

Учитывая тот факт, что максимальный радиус первая зона Френеля имеет в точке, равноудаленной от обеих антенн, получим упрощенную формулу для его вычисления:

$$R = 17,32 \sqrt{\frac{D}{4F}},$$

где D — расстояние между антеннами, км.

В ряде источников утверждается, что если внутри окружности с радиусом примерно 0,6 радиуса первой зоны Френеля, проведенной вокруг любой точки радиолинии, нет никаких преград, то затуханием сигнала, обусловленным наличием преград, можно пренебречь. Другими словами, если в области, радиус которой составляет 60 % первой зоны Френеля, нет преград, то при расчете радиолинии можно ограничиться только учетом потерь сигнала в свободном пространстве. Для достижения этого высота подвеса антенн приемника и передатчика должна быть такой, чтобы вдоль радиолинии не было ни одной точки, расстояние от которой до препятствия было бы меньше, чем 0,6 радиуса первой зоны Френеля. Следует учитывать, что поверхность земли также является одним из препятствий.

Для упрощенного вычисления радиуса области, составляющего 60 % радиуса первой зоны Френеля, умножим выражение предыдущей формулы на коэффициент 0,6:

$$R(60\%) = 10,4 \sqrt{\frac{D}{4F}}.$$

Другие источники устанавливают более жесткие требования: преграды должны отсутствовать в 80 % первой зоны Френеля. Для упрощенного вычисления радиуса области, составляющего 80 % радиуса первой зоны Френеля, нужно умножить выражение для упрощенного вычисления максимального радиуса первой зоны Френеля на коэффициент 0,8:

$$R(80\%) = 13,86 \sqrt{\frac{D}{4F}}.$$

Следует понимать, что радиус первой зоны Френеля не является высотой установки антенн, но используется для ее вычисления, при котором необхо-

можно учитывать также кривизну земной поверхности (рис. 6.6), рассчитанную по формуле

$$H_{\text{earth}} = \frac{D^2}{68},$$

где H_{earth} — кривизна земной поверхности, м.

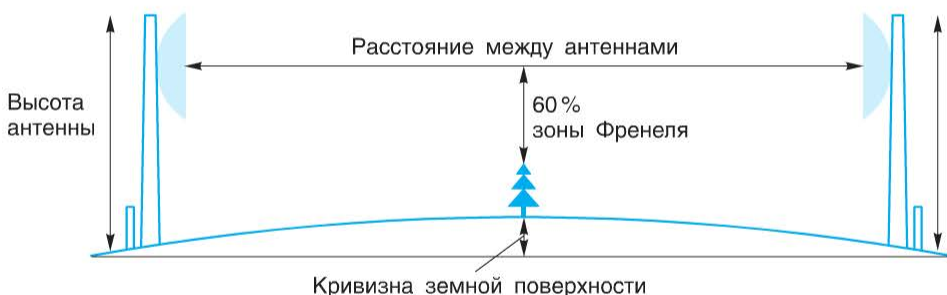


Рис. 6.6. Определение высоты установки антенн

В таком случае минимальная высота установки антенн над препятствиями с учетом того, что 60 % первой зоны Френеля свободно от преград, будет вычисляться по формуле

$$H_{\text{ant}} = 10,4 \sqrt{\frac{D}{4F}} + \frac{D^2}{68}.$$

При расчете высоты установки антенны с учетом отсутствия препятствий в 80 % первой зоны Френеля коэффициент 10,4 в последней формуле заменяют на 13,86.

Приведем пример расчета радиуса первой зоны Френеля, если расстояние между антеннами 2 км, передача ведется в диапазоне 2,4 ГГц на канале 6 (2437 МГц):

$$R = 17,32 \sqrt{\frac{2}{4 \cdot 2,437}} = 7,84 \text{ м.}$$

Минимальная высота установки антенн с учетом того, чтобы 60 % первой зоны Френеля было свободно от препятствий:

$$H_{\text{ant}} = 10,4 \sqrt{\frac{2}{4 \cdot 2,437}} + \frac{2^2}{68} = 4,76 \text{ м.}$$

Минимальная высота установки антенн с учетом того, чтобы 80 % первой зоны Френеля было свободно от препятствий:

$$H_{\text{ant}} = 13,86 \sqrt{\frac{2}{4 \cdot 2,437}} + \frac{2^2}{68} = 6,34 \text{ м.}$$

Сторона приемника

Чувствительность приемника (receiver sensitivity) — параметр, определяющий минимальный уровень сигнала на входе и позволяющий приемнику демодулировать сигнал с определенным допустимым уровнем ошибок. Эта величина является одним из важнейших параметров оценки характеристик оборудования Wi-Fi, который определяет достижимые скорости передачи данных и дальность связи. Чувствительность приемника указывается для конкретной скорости передачи, поскольку каждая схема модуляции имеет свои требования к отношению сигнал/шум. Измеряется чувствительность в дБм со знаком «—». Чем она ниже, тем лучше приемник и больше дальность связи.

Таблица 6.4. Требования к приемнику в спецификации 802.11n

Диапазон, МГц	Модуляция	Чувствительность приемника при пакетной ошибке $\leq 10\%$ и длине пакета 4096 байт, дБм	
		Канал 20 МГц	Канал 40 МГц
2400–2483,5 5150–5350 5650–6425	BPSK 1/2	–82	–79
	QPSK 1/2	–79	–76
	QPSK 3/4	–77	–74
	16-QAM 1/2	–74	–71
	16-QAM 3/4	–70	–67
	64-QAM 2/3	–66	–63
	64-QAM 3/4	–65	–62
	64-QAM 5/6	–64	–61

Требования к чувствительности приемников оборудования 802.11n в соответствии со стандартом приведены в табл. 6.4, а параметры чувствительности приемника точки доступа D-Link DAP-2310 для разных стандартов — в табл. 6.5.

Способность приемника обеспечивать прием радиоволн («чувствовать» их) зависит от наличия рядом нежелательных сигналов (шумов), взаимодействующих с исходной волной. Шум является одним из основных факторов, ограничивающих производительность линии связи. Напомним, что максимальная пропускная способность зависит от полосы пропускания канала связи и отношения сигнал/шум (SNR). Чем больше скорость передачи, тем больший ущерб может нанести нежелательный шум, поскольку при этом возрастает скорость возникновения ошибок.

Отношение сигнал/шум определяется как отношение мощности сигнала к мощности шума (помех) и выражается в децибелах (дБ). Как правило, данное соотношение измеряется в приемнике, так как именно в этой точке обрабатывается сигнал и устраняется нежелательный шум. Чем больше отношение сигнал/шум, тем меньше шум влияет на полезный сигнал при его передаче по каналу связи, что приводит к хорошему распознаванию сигнала

приемником. Отношение сигнал/шум изменяется во времени, так как источники шумов могут появляться или исчезать, например при включении и отключении микроволновой печи.

Таблица 6.5. Чувствительность приемника D-Link DAP-2310

IEEE 802.11b	IEEE 802.11g	IEEE 802.11n (в зависимости от ширины канала)
<div>–76 dBm при 1 Мбит/с</div> <div>–76 dBm при 2 Мбит/с</div> <div>–76 dBm при 5,5 Мбит/с</div> <div>–76 dBm при 11 Мбит/с</div>	<div>–82 dBm при 6 Мбит/с</div> <div>–81 dBm при 9 Мбит/с</div> <div>–79 dBm при 12 Мбит/с</div> <div>–77 dBm при 18 Мбит/с</div> <div>–74 dBm при 24 Мбит/с</div> <div>–70 dBm при 36 Мбит/с</div> <div>–66 dBm при 48 Мбит/с</div> <div>–65 dBm при 54 Мбит/с</div>	<div>HT20</div> <div>–82dBm при MCS0</div> <div>–79dBm при MCS1</div> <div>–77dBm при MCS2</div> <div>–74dBm при MCS3</div> <div>–70dBm при MCS4</div> <div>–66dBm при MCS5</div> <div>–65dBm при MCS6</div> <div>–64dBm при MCS7</div> <div>HT40</div> <div>–82dBm при MCS0</div> <div>–79dBm при MCS1</div> <div>–77dBm при MCS2</div> <div>–74dBm при MCS3</div> <div>–70dBm при MCS4</div> <div>–66dBm при MCS5</div> <div>–65dBm при MCS6</div> <div>–64dBm при MCS7</div>

Одной из серьезных проблем, с которой сталкиваются проектировщики беспроводных сетей, является *замирание сигнала (fading)* — изменение мощности полученного сигнала во времени, вызванное изменением линии связи или среды распространения. Замирание сигнала в беспроводных сетях может быть вызвано многолучевым распространением или изменением в атмосфере, например наличием или отсутствием дождя или снега. Замирания сигнала можно условно разделить на быстрые и медленные. Быстрыми являются временные изменения амплитуды принимаемого сигнала, связанные с интерференцией прямой и отраженной волн от поверхности Земли или других предметов, неоднородностью атмосферы; медленные определяются в основном дневными или сезонными ослаблениями радиосигнала, а также наличием перемещающихся на местности предметов (например, в уличных беспроводных сетях человек может проходить мимо зданий разной высоты, деревьев и т. п.). Надежность работы беспроводной линии связи в первую очередь определяется энергетическим запасом на компенсацию быстрых и медленных замираний. При расчетах линии связи предусматривают резерв на компенсацию этих замираний — *запас на замирание сигнала (SOM, System*

Operating Margin), который определяется как разница между уровнем фактически принимаемого сигнала и чувствительностью приемника, зависящей от выбранного типа модуляции:

$$SOM = P_{tr} - L_{tr} + G_{tr} - L_{bf} + G_{recv} - L_{recv} - P_{recv}.$$

Чем выше значение *SOM*, тем надежнее беспроводная линия связи. Считается, что минимальная величина запаса на замирание должна быть не меньше 10 дБ и этого достаточно для инженерного расчета, но на практике зачастую используют значение 20...30 дБ.

6.2. Пример расчета линии связи

Оценим возможность работы канала связи длиной 2 км между точкой доступа D-Link DAP-3310 и беспроводным клиентом с адаптером D-Link DWA-182 на максимальной скорости, поддерживаемой беспроводной сетью (300 Мбит/с). Устройства работают на канале 6 (центральная частота 2437 МГц).

Исходные данные:

- мощность передатчика DAP-3310 на всех скоростях: 20 dBm;
- мощность передатчика DWA-182 на скорости 300 Мбит/с: 15 dBm;
- мощность передатчика DWA-182 на скорости 1 Мбит/с: 19 dBm;
- чувствительность DAP-3310 на скорости 300 Мбит/с: -69 dBm;
- чувствительность DAP-3310 на скорости 1 Мбит/с: -96 dBm;
- чувствительность DWA-182 на скорости 300 Мбит/с: -61 dBm;
- чувствительность DWA-182 на скорости 1 Мбит/с: -87 dBm;
- коэффициент усиления штатной антенны DAP-3310: 10 dBi;
- коэффициент усиления штатной антенны DWA-182: 0 dBi;
- потерь в антенно-фидерном тракте (между беспроводными устройствами и их антеннами) нет (0 дБм).

Оценим линию связи в направлении от точки доступа к клиенту.

Найдем потери в свободном пространстве:

$$20 \lg(2437) + 20 \lg(2) + 32,4 = 106,1 \text{ дБ.}$$

Рассчитаем запас на замирание для скорости 300 Мбит/с:

$$SOM = 20 - 0 + 10 - 106,1 + 0 - 0 - (-61) = -15,1 \text{ дБ.}$$

Оценим линию связи в обратном направлении — от клиента к точке доступа.

Значение потерь в свободном пространстве не изменится.

Рассчитаем запас на замирание:

$$SOM = 15 - 0 + 0 - 106,1 + 10 - 0 - (-69) = -12,1 \text{ дБ.}$$

Как видно из приведенных расчетов, запас на замирание линии связи в обоих направлениях намного меньше 10 дБм, что говорит о ее недостаточном энергетическом потенциале.

Решим обратную задачу и определим максимальное расстояние, на котором линия связи между DAP-3310 и DWA-182 будет стабильно работать в обоих направлениях при скоростях передачи 300 Мбит/с и 1 Мбит/с.

Формула для расчета дальности связи получается из выражения для потерь в свободном пространстве:

$$D = 10^{\left(\frac{L_{bf} - 20 \lg F - K}{20} \right)}.$$

Исходя из полного уравнения энергетического потенциала линии связи, потери в свободном пространстве можно вычислить следующим образом:

$$L_{bf} = P_{tr} - L_{tr} + G_{tr} + G_{recv} - L_{recv} - P_{recv} - SOM.$$

Найдем расстояние между устройствами при передаче данных на скорости 300 Мбит/с. Передающее устройство — DAP-3310, принимающее устройство — DWA-182. Значение SOM при расчетах будем брать равным 10 дБ.

Потери в свободном пространстве составят:

$$L_{bf} = 20 - 0 + 10 + 0 - 0 - (-61) - 10 = 81 \text{ дБ}.$$

По приведенной выше формуле находим дальность связи:

$$D = 10^{\left(\frac{81 - 20 \lg(2437) - 32,4}{20} \right)} = 0,111 \text{ км} = 111 \text{ м}.$$

Сделаем расчет для обратного направления линии связи. Передающее устройство — DWA-182, принимающее устройство — DAP-3310.

Потери в свободном пространстве:

$$L_{bf} = 15 - 0 + 0 + 10 - 0 - (-69) - 10 = 84 \text{ дБ}.$$

Дальность связи:

$$D = 10^{\left(\frac{84 - 20 \lg(2437) - 32,4}{20} \right)} = 0,157 \text{ км} = 157 \text{ м}.$$

Таким образом, максимальное расстояние между устройствами, при котором они будут стабильно работать на скорости 300 Мбит/с, составляет не более 111 метров.

Найдем расстояние между устройствами при передаче данных на скорости 1 Мбит/с. Передающее устройство — DAP-3310, принимающее устройство — DWA-182.

Потери в свободном пространстве:

$$L_{bf} = 20 - 0 + 10 + 0 - 0 - (-87) - 10 = 107 \text{ дБ}.$$

Дальность связи:

$$D = 10^{\left(\frac{107 - 20 \lg(2437) - 32,4}{20} \right)} = 2,2 \text{ км}.$$

Сделаем расчет для обратного направления линии связи. Передающее устройство — DWA-182, принимающее устройство — DAP-3310.

Потери в свободном пространстве:

$$L_{bf} = 19 - 0 + 0 + 10 - 0 - (-96) - 10 = 115 \text{ дБ.}$$

Дальность связи:

$$D = 10^{\left(\frac{115 - 20 \lg(2437) - 32,4}{20} \right)} = 5,6 \text{ км.}$$

Таким образом, максимальное расстояние между устройствами, при котором они будут стабильно работать на скорости 1 Мбит/с, составляет не более 2,2 км.

7. Проектирование беспроводных сетей

Существуют различные подходы к проектированию беспроводных сетей. Целью одних является обеспечение максимальной зоны охвата, других — достижение максимальной производительности передачи данных, третьих — нахождение баланса между зоной охвата и производительностью. Поэтому полезно понимать, какие подходы в каких случаях применимы при проектировании сетей.

Проектирование беспроводной сети, сфокусированное на достижении максимальной зоны покрытия, используется в случае небольшого числа беспроводных клиентов. Целями при этом являются обеспечение достаточной мощности радиосигнала только в тех местах, где требуется беспроводной доступ, достижение максимальной зоны покрытия вокруг каждой точки доступа, уменьшение общего количества точек доступа для снижения затрат. Планирование производительности в данном случае не выполняется, так как плотность устройств и требования к производительности достаточно низкие. Такой подход к проектированию оправдывает себя до тех пор, пока плотность беспроводных устройств остается низкой и подходит для проектирования беспроводных сетей складов, предприятий розничной торговли, мест общего пользования с небольшим количеством клиентов.

Однако по мере увеличения количества и типов потребительских мобильных устройств, дающих сотрудникам возможность работать с ресурсами компании, используя любое *собственное мобильное устройство (Bring-Your-Own-Device, BYOD)*, беспроводные сети превращаются в основное средство доступа к корпоративным сетям и нагрузка на них увеличивается.

Сетевая структура с высокой плотностью беспроводных клиентов требует проектирования беспроводных сетей, направленных на достижение высокой производительности. При таком подходе к проектированию особое внимание уделяется технологии *повторного использования частоты (frequency reuse technique)*, что достигается за счет небольших ячеек (выходную мощность точек доступа ограничивают так, чтобы зона покрытия находилась в заданном физическом пространстве), направленных антенн и тщательного контроля параметров канала и мощности излучения. Однако этот подход обычно предполагает высокую стоимость проекта за счет использования большого количества точек доступа и сопутствующего оборудования и требует высокой квалификации персонала, разрабатывающего и обслуживающего сеть. Поэтому он редко применяется, например, при проектировании пресс- и конференц-центров и других публичных мест с высокой плотностью беспроводных клиентов.

Подход к проектированию, представляющий собой нечто среднее между вышеописанными подходами, нацелен на достижение баланса между максимальной зоной покрытия и высокой производительностью. Он предполагает четкий анализ требований к производительности сети, для того чтобы определить оптимальное количество точек доступа, позволяющее удовлетворить

текущие и будущие потребности. Повторное использование частот критически важно при радиочастотном планировании, так как это позволит избежать значительной межканальной интерференции (CCI) при требуемой плотности точек доступа. Сбалансированный подход к проектированию подходит для большинства современных беспроводных сетей, которые сталкиваются с увеличивающимся количеством беспроводных клиентов и используют WLAN в качестве основного метода доступа к корпоративным сетям.

7.1. Этапы проектирования беспроводной сети

Для того чтобы спрогнозировать требования к производительности беспроводной сети, многие проектировщики используют грубую оценку, основанную на количестве пользователей, количестве устройств на одного пользователя и желаемом лимите клиентских устройств на одну точку доступа. Этот метод не отражает точную потребность в производительности и не включает в себя радиочастотное планирование. Поэтому зачастую возникают ситуации, когда при использовании большого количества точек доступа требуемая производительность не достигается из-за неучтенного негативного влияния на нее межканальной интерференции.

Планирование производительности беспроводной сети должно быть связано с радиочастотным планированием для того, чтобы определить требуемое количество точек доступа, места их размещения, используемые ими каналы и антенны, а также итоговую зону покрытия.

Процесс разработки или расширения беспроводной сети обычно включает несколько стандартных шагов.

1. **Формулировка целей создания беспроводной сети:** определение участников проекта, критериев оценки достижения целей, существующих и новых бизнес-процессов.

2. **Сбор информации:** о характеристиках сетевой инфраструктуры, характеристиках и моделях клиентских устройств, определение требований приложений к производительности сети и задержке при передаче.

3. **Планирование производительности беспроводной сети:** выполнение предварительной оценки производительности на основе расчета времени передачи для уникальных комбинаций клиентов и приложений WLAN.

4. **Планирование зоны покрытия:** выполнение предварительного обследования места развертывания беспроводной сети, которое включает проведение измерений радиочастотных характеристик среды и проведение различных тестов, моделирование зон покрытия с помощью планировщика беспроводных сетей, например D-Link Wi-Fi Planner PRO.

5. **Развертывание беспроводной сети (установка и настройка оборудования):** интеграция с сервисами проводной сети (коммутаторы/маршрутизаторы, организация питания с помощью PoE, IP-адресация, подключение к Интернет), обеспечение сервисов мобильным пользователям (роуминг, туннелирование, mobile IP), обеспечение безопасности сети и данных через AAA (*Authentication, Authorization, Accounting*), сегментация беспроводной сети,

гостевые сервисы, интеграция со службами каталогов (*Active Directory*), управление конфигурацией сети, обеспечение отказоустойчивости, обеспечение мониторинга, поиска неисправностей и регистрации событий через систему сетевого управления (например, с помощью D-Link D-View).

6. Тестирование зоны охвата: определение зоны покрытия сети, выполнение анализа спектра для обнаружения и исключения источников интерференции.

7.2. Сбор информации о клиентских устройствах

Сбор информации о количестве, типах и функциональных возможностях устройств, подключенных к сети, является одной из важных частей процесса проектирования. В последние годы клиентские устройства с поддержкой 802.11n практически вытеснили устройства 802.11a/b/g, также расширяется парк клиентских устройств с поддержкой интерфейса 802.11ac.

Сетевому администратору не составляет труда получить информацию о количестве и типе устройств, используемых в сети и принадлежащих компании. Однако в последнее время набирает популярность концепция *Bring-Your-Own-Device (BYOD)*, в рамках которой сотрудникам позволяется работать с ресурсами компании, используя любое собственное мобильное устройство, будь то ноутбук, нетбук, планшет или смартфон, и получая при этом доступ к нужным папкам и данным.

Устройства, принадлежащие компании, соответствуют корпоративной политике, включая политику безопасности, поэтому не возникает проблем с их совместимостью, осуществлением контроля над ними, а также заменой или ремонтом при выходе из строя. Если сотрудник использует свое мобильное устройство в корпоративных целях, беспроводная сеть должна уметь выделять трафик такого устройства, чтобы идентифицировать и зарегистрировать это устройство в сети. Администратор сети практически не имеет контроля над такими устройствами, что может приводить к проблемам с их безопасностью и совместимостью.

Еще один тип устройств, которые могут подключаться к корпоративной сети — гостевые устройства. Их обычно приносят посетители или партнеры. В этом случае администратор может организовать гостевой доступ к сети с ограниченными правами.

Сотрудники могут использовать в своей работе более одного беспроводного устройства, например ноутбук и планшет, что также следует учитывать при определении количества устройств в сети.

Кроме этого требуется определить количество клиентских устройств, способных работать только в одном диапазоне частот и в обоих одновременно. Эти данные необходимо учитывать при построении беспроводной инфраструктуры и выборе частотного диапазона BSS.

Для того чтобы добиться максимально высокой производительности сети, наряду с количеством устройств необходимо определить приложения, ис-

пользуемые клиентами, а также предъявляемые ими требования к пропускной способности и качеству обслуживания (QoS).

Определить потребность приложений в пропускной способности можно с помощью любого анализатора сетевого трафика. Для справки приведем перечень типовых сетевых приложений с указанием их требований к пропускной способности и классификацией по категориям доступа WMM (табл. 7.1). Напомним, что WMM обеспечивает классификацию трафика на основе восьми уровней приоритетов, которые привязываются к четырем категориям доступа: voice, video, best effort, background. Эти четыре категории доступа, в свою очередь, привязываются к четырем очередям QoS.

Таблица 7.1. Требования приложений к пропускной способности

Приложение	Требуемая пропускная способность	Категория доступа WMM
VoIP — передача голоса	27–93 Кбит/с (зависит от кодека)	Voice (VO)
VoIP — сигнализация (SIP)	5 Кбит/с	Best effort (BE)
Web-конференции	384 Кбит/с–1 Мбит/с	Video (VI)
Видео высокой четкости (сжатое)	20–50 Мбит/с	Video (VI)
Видео высокой четкости (слабо сжатое)	70–200 Мбит/с	Video (VI)
Видео высокой четкости (несжатое)	1,3–3 Гбит/с	Video (VI)
Видео стандартной четкости	1–1,5 Мбит/с	Video (VI)
E-mail/просмотр Web-страниц	0,5–1 Мбит/с	Best effort (BE)
Загрузка файлов	5 Мбит/с	Best effort (BE)
YouTube	0,9 Мбит/с	Best effort (BE)
Сетевое резервное копирование	Вся доступная полоса	Background (BK)

Приведенные требования приложений к пропускной способности могут использоваться для грубой оценки требований к скорости передачи точки доступа.

В случае если бóльшую долю передаваемого трафика составляет высокоприоритетный голосовой и видеотрафик, то в сети следует использовать оборудование с поддержкой функции *admission control*, являющейся удобным средством управления полосой пропускания в беспроводных сетях с высокой загрузкой и улучшающей их производительность при передаче видео и голоса. Эта функция использует протокол *Traffic Specification* (TSPEC) для обеспечения сигнализации между точкой доступа и клиентским устройством. При задействовании этой функции клиентское устройство отправляет точке доступа запрос на доступ к каналу для передачи трафика из высокоприоритетной очереди (согласно категориям доступа WMM). Точка доступа оценивает сетевую загрузку и состояние канала с учетом запроса клиента. Если точка

доступа удовлетворяет запрос, она выделяет клиенту полосу пропускания для передачи потока данных. Если запрос отвергается, клиент не может начать передачу высокоприоритетного потока данных. Для того чтобы функция *admission control* работала, она должна поддерживаться как на точке доступа, так и на клиентском устройстве (рис. 7.1).

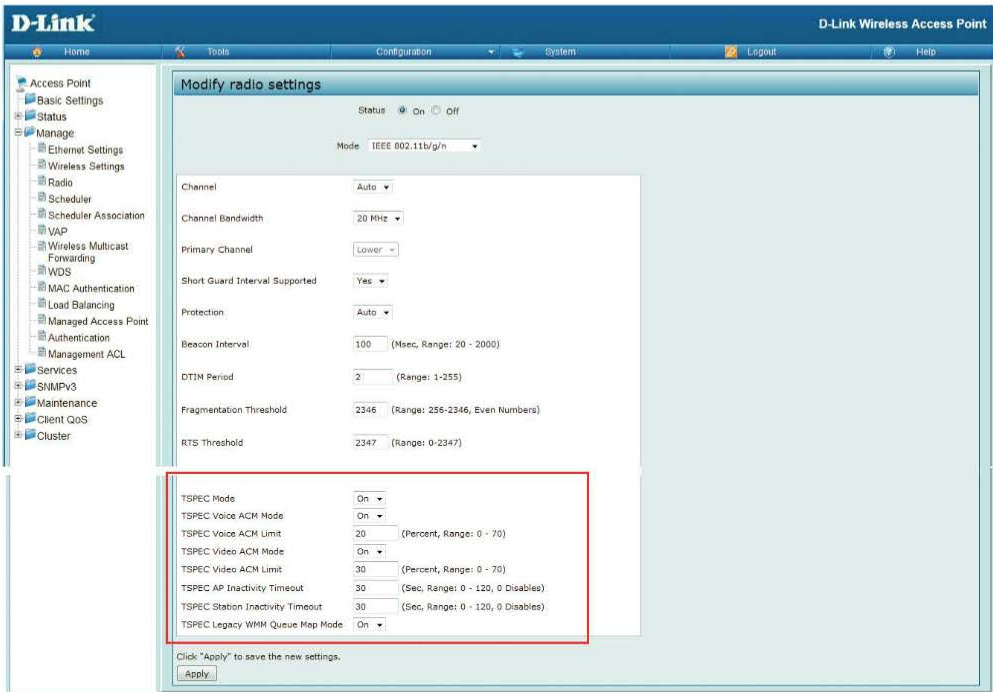


Рис. 7.1. Настройка функции *admission control* на точке доступа

Функция *admission control* в устройствах разных производителей может быть реализована по-разному. Для того чтобы обеспечить их совместимость, Wi-Fi Alliance ввел программу сертификации Wi-Fi CERTIFIED WMM-Admission Control.

7.3. Планирование производительности и зоны охвата беспроводной сети

Планирование производительности беспроводной сети должно быть связано с радиочастотным планированием вследствие необходимости определения требуемого количества точек доступа, мест их расположения, типов антенн, номеров каналов для достижения необходимой зоны покрытия. Поскольку производительность и дальность действия беспроводных сетей не безграничны, при их проектировании следует учитывать множество параметров (частота, скорость передачи, мощность излучения и т. д.), которые на

них влияют. Например, увеличивая скорость передачи и переходя из диапазона 2,4 ГГц в 5 ГГц, производительность при прочих равных условиях будет увеличиваться, а дальность действия уменьшаться. При другом подходе можно повысить мощность излучения передатчика и задействовать антенну с большим коэффициентом усиления, увеличив при этом и дальность действия, и производительность.

7.3.1. Скорость передачи данных и пропускная способность

Скорость передачи данных (data rate), которая обычно указывается в характеристиках беспроводных устройств, является максимально возможной теоретической пропускной способностью сети, достигаемой при использовании конкретной технологии. Реальная пропускная способность, однако, всегда меньше теоретической, что связано с издержками на передачу служебной информации, количеством клиентов, расстоянием, наличием преград, интерференцией и многими другими факторами. Поддержание надежной работы и безопасности беспроводной сети снижает теоретическую скорость передачи данных примерно на 30...50 % (рис. 7.2).

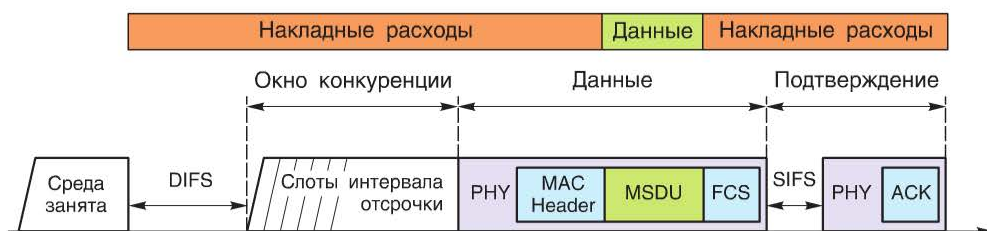


Рис. 7.2. Накладные расходы при передаче кадра

Не стоит забывать, что беспроводная среда является разделяемой (совместно используемой): передачи происходят в режиме полудуплекса, когда только одно устройство в один момент времени может использовать канал. Поэтому чем больше клиентских устройств подключается к каналу, тем больше трафика они создают и тем меньше реальная скорость передачи.

Для грубой оценки средней пропускной способности, приходящейся на одно соединение, при использовании соответствующей спецификации 802.11 можно воспользоваться следующей формулой:

$$\text{Average Throughput} = (\text{DataRate} \div 2) \div n,$$

где *Average Throughput* — средняя пропускная способность на одного клиента; *DataRate* — скорость передачи данных конкретной спецификации 802.11; *n* — количество беспроводных клиентов, подключенных к сети.

Данная формула предполагает, что точка доступа и клиентское устройство используют одну и ту же спецификацию 802.11 и конфигурацию. Падение скорости передачи при удалении клиента от точки доступа, требования

приложений к пропускной способности, влияние интерференции и других факторов, происходящих в реальной сети, не учитывается.

Приведем пример падения средней пропускной способности беспроводной сети на одного клиента при увеличении их количества (табл. 7.2).

Таблица 7.2. Скорость передачи данных и средняя пропускная способность на одного клиента

Спецификация	Скорость передачи данных, Мбит/с	Средняя пропускная способность*, Мбит/с	Количество клиентов	Средняя пропускная способность на одного клиента, Мбит/с
802.11g	54	24	10	2,4
802.11a	54	24	20	1,2
802.11n (1x1, 20 МГц, short guard interval)	72,2	36,1	10	3,61
802.11n (1x1, 40 МГц, short guard interval)	150	75	20	3,75
802.11n (2x2, 20 МГц, short guard interval)	144,4	72,2	10	7,22
802.11n (2x2, 40 МГц, short guard interval)	300	150	10	15
802.11n (2x2, 40 МГц, short guard interval)	300	150	20	7,5
802.11ac (2x2, 80 МГц, short guard interval)	866,7	433,5	10	43,35
802.11ac (2x2, 80 МГц, short guard interval)	866,7	433,5	15	28,9
802.11ac (2x2, 80 МГц, short guard interval)	866,7	433,5	20	21,7
802.11ac (3x3, 80 МГц, short guard interval)	1300	650	10	65
802.11ac (3x3, 80 МГц, short guard interval)	1300	650	30	21,7

* В предположении 50 %-ного падения скорости (клиенты 802.11a/g являются исключением из-за отсутствия поддержки технологии агрегации кадров).

Еще одной причиной падения производительности является различие скоростей ассоциации при подключении клиентов разных спецификаций к точке доступа. Например, если к точке доступа 802.11n подключается кли-

ент 802.11g, то точка доступа будет вынуждена передавать данные на максимальной для этого клиента скорости, иначе он не сможет демодулировать сигнал. Если к точке доступа будет подключено множество низкоскоростных клиентов, ее средняя пропускная способность значительно падает. При выполнении одних и тех же приложений «низкоскоростные» клиенты занимают канал в течение большего времени, чем «высокоскоростные».

Примерное время, требуемое клиенту для передачи трафика соответствующего приложения через канал, можно определить с помощью следующей формулы:

$$\text{Airtime Utilization} = (\text{Application Throughput} \cdot 100\%) / (\text{Device Throughput}),$$

где *Airtime Utilization* — время использования канала в %; *Application Throughput* — потребность приложения в пропускной способности; *Device Throughput* — пропускная способность устройства с учетом издержек на передачу и факторов внешней среды.

Предположим, что к точке доступа 802.11n (2x2, 40 МГц, 300 Мбит/с) в диапазоне 2,4 ГГц подключены клиент 802.11n (2x2, 40 МГц, 300 Мбит/с) и клиент 802.11g (1x1, 20 МГц, 54 Мбит/с). Оценим время, необходимое каждому клиенту для загрузки файлов. Пропускная способность, требуемая приложению — 5 Мбит/с. Для передачи данных используется канал шириной 20 МГц. Напомним, что скорость передачи двух пространственных потоков при ширине канала 20 МГц в 802.11n равна 144,4 Мбит/с. Для простоты вычислений будем считать, что средняя пропускная способность устройств в 2 раза меньше максимальной скорости передачи данных.

$$\text{Клиент 802.11n: } (5 \text{ Мбит/с} \cdot 100 \%) / (72,2 \text{ Мбит/с}) = 6,9 \%.$$

$$\text{Клиент 802.11g: } (5 \text{ Мбит/с} \cdot 100 \%) / (24 \text{ Мбит/с}) = 20,8 \%.$$

С учетом различных накладных расходов, связанных с отправкой служебных сообщений приложения, время использования канала по факту будет в 2 раза больше. Таким образом, клиенту 802.11n на загрузку файлов потребуется 13,8 % канального времени, а клиенту 802.11g — 41,6 %. Как видно из расчетов, «низкоскоростному» клиенту требуется в 3 раза больше времени при выполнении аналогичного приложения. Занимая больше канального времени, «низкоскоростные» клиенты «крадут» канальное время у «высокоскоростных», что, в свою очередь, приводит к перегрузке сети, снижению ее производительности и повышению средней задержки передачи. Это может сказаться на качестве передачи голоса, видео и других чувствительных к задержкам приложений.

Одним из решений данной проблемы является использование двухдиапазонных точек доступа с поддержкой одновременной передачи в обоих диапазонах. Два разных диапазона позволяют создать две физически независимые беспроводные сети. «Низкоскоростных» клиентов при этом можно

подключать в диапазоне 2,4 ГГц, а «высокоскоростных» — в диапазоне 5 ГГц (рис. 7.3). Клиенты, настроенные на ассоциацию с сетью 2,4 ГГц, не будут мешать клиентам, настроенным на ассоциацию с сетью 5 ГГц. Таким образом повышается общая производительность сети.



Рис. 7.3. Физическое разделение низкоскоростных и высокоскоростных клиентов

Вернемся к рассмотренному выше примеру и проверим изменение времени использования канала клиентом 802.11n, если он будет подключен к точке доступа в диапазоне 5 ГГц. В этом случае и клиент, и точка доступа смогут использовать канал шириной 40 МГц.

Клиент 802.11n в диапазоне 5 ГГц: $(5 \text{ Мбит/с} \cdot 100 \%) / (150 \text{ Мбит/с}) = 3,4 \%$.

Таким образом, при работе клиента 802.11n в диапазоне 5 ГГц время использования канала уменьшается почти в 2 раза. Следствием уменьшения канального времени является возможность подключения к точке доступа дополнительных клиентов или выделение большего времени на передачу уже ассоциированным клиентам.

Как определить количество точек доступа, требуемое для обслуживания всех клиентов сети? В зависимости от модели точка доступа может поддерживать подключение до 200 пользователей. Но сможет ли в этом случае точка доступа обеспечить требуемую производительность?

Одним из первых шагов при проектировании беспроводной сети является сбор информации о клиентах: их количестве, конфигурации и выполняемых приложениях. Пример записи информации о клиентах приведен в табл. 7.3.

Таблица 7.3. Запись информации о клиентах

Клиентское устройство	Приложение	Количество устройств	Ассоциировано / активно	Требования приложения к пропускной способности
Ноутбук (11n, 1x1, 40 МГц, 2,4 ГГц)	Web Browsing & E-mail	10	Одновременно ассоциировано и активно	500 Кбит/с
	Skype standard definition video call			600 Кбит/с
	File Sharing			5 Мбит/с
ПК (11n, 2x2, 40 МГц, 2,4/5 ГГц)	Web Browsing & E-mail	30	Одновременно ассоциировано и активно	500 Кбит/с
	Skype standard definition video call			600 Кбит/с
	File Sharing			5 Мбит/с

Далее определяем базовые характеристики точки доступа и выбираем модель устройства, выбираем частотный диапазон, определяем ширину канала в каждом диапазоне (в диапазоне 2,4 ГГц рекомендуется использовать каналы 20 МГц), определяем желаемый лимит клиентских устройств на одну точку доступа (рекомендуется подключать к одной точке не более 15–20 устройств, даже если она может поддерживать значительно большее число клиентов), определяем распределение клиентов между диапазонами.

Рассмотрим два примера. В первом примере сеть строится на точках доступа, работающих только в диапазоне 2,4 ГГц, во втором — работающих в диапазонах 2,4 и 5 ГГц одновременно.

Пример 1: для построения беспроводной сети возьмем точку доступа 802.11n модели D-Link DAP-2330. Она работает в диапазоне 2,4 ГГц на скорости 300 Мбит/с. Характеристики инфраструктуры: рабочий диапазон сети 2,4 ГГц, ширина канала 20 МГц, максимальное количество клиентов на одну точку доступа — 15. Информация о клиентах приведена в табл. 7.3. Требуется рассчитать количество точек доступа DAP-2330, требуемых для построения сети.

1. Определяем канальное время для каждого типа клиентских устройств и каждого типа приложений, выполняющихся на них. Для клиентского ноутбука (11n, 1x1, 40 МГц), подключенного к точке доступа в диапазоне 2,4 ГГц и использующего канал шириной 20 МГц, максимальная скорость передачи данных составит 72,2 Мбит/с. Для простоты вычислений будем считать, что средняя пропускная способность в 2 раза меньше максимальной скорости передачи данных и равна $72,2 \text{ Мбит/с} \div 2 = 36,1 \text{ Мбит/с}$. Примерное время, требуемое клиенту для загрузки файлов (*File Sharing*) через канал, будет равно: $(5 \text{ Мбит/с} \cdot 100 \%) \div 36,1 \text{ Мбит/с} = 13,85 \%$. Учтем накладные расходы, связанные с отправкой служебных сообщений приложения, и увеличим вычисленное время в 2 раза: $13,85 \% \cdot 2 = 27,7 \%$. Аналогичным образом опре-

деляем время использования канала для каждого типа клиентских устройств и каждого типа приложений, выполняющихся на них. Результаты вычислений приведены в табл. 7.4.

Таблица 7.4. Рассчитанное канальное время для примера 1

Клиентское устройство	Приложение	Канальное время 2,4 ГГц (20 МГц)
Ноутбук (11n, 1x1, 40 МГц, 2,4 ГГц)	Web Browsing & Email	2,77 %
	Skype standard definition video call	3,24 %
	File Sharing	27,7 %
Итого:		33,71 %
ПК (11n, 2x2, 40 МГц, 2,4/5 ГГц)	Web Browsing & Email	1,38 %
	Skype standard definition video call	1,66 %
	File Sharing	13,8 %
Итого:		16,84 %

2. Определяем количество точек доступа, требуемое для обслуживания каждого клиента. Для этого умножаем количество устройств каждого типа на суммарную долю использования канала. Для обслуживания 10 ноутбуков потребуется примерно $10 \cdot 0,3371 \approx 4$ точки доступа. Для обслуживания 30 ПК с беспроводным адаптером потребуется примерно $30 \cdot 0,1684 \approx 5$ точек доступа.

3. Определяем суммарное количество точек доступа. Для этого надо сложить количество точек доступа, требуемое для обслуживания клиентов каждого типа. Для построения беспроводной сети в диапазоне 2,4 ГГц, состоящей из 10 ноутбуков и 30 ПК, необходимо $4 + 5 = 9$ точек доступа DAP-2330. Если в будущем планируется расширение сети, то количество точек доступа надо увеличить в соответствующее число раз.

Пример 2: для построения беспроводной сети возьмем точку доступа 802.11ac модели D-Link DAP-2660. Она работает в диапазоне 2,4 ГГц на скорости 300 Мбит/с, в диапазоне 5 ГГц — на скорости 866,7 Мбит/с. Характеристики инфраструктуры: рабочий диапазон сети 2,4 и 5 ГГц, ширина канала 20 МГц (2,4 ГГц) и 40 МГц (5 ГГц), максимальное количество клиентов на одну точку доступа — 15, «высокоскоростные» клиенты подключаются к точке доступа в диапазоне 5 ГГц. Информация о клиентах приведена в табл. 7.3. Рассчитаем количество точек доступа DAP-2660, требуемых для построения сети.

1. Определяем канальное время для каждого типа клиентских устройств и каждого типа приложений, выполняющихся на них. Результаты вычислений приведены в табл. 7.5.

Таблица 7.5. Рассчитанное канальное время для примера 2

Клиентское устройство	Приложение	Канальное время	
		2,4 ГГц (20 МГц)	5 ГГц (40 МГц)
Ноутбук (11n, 1x1, 40 МГц, 2,4 ГГц). Ноутбук может работать только в диапазоне 2,4 ГГц	Web Browsing & Email	2,77 %	—
	Skype standard definition video call	3,24 %	—
	File Sharing	27,7 %	—
Итого:		33,71 %	—
ПК (11n, 2x2, 40 МГц, 2,4/5 ГГц)	Web Browsing & Email	1,38 %	0,67 %
	Skype standard definition video call	1,66 %	0,8 %
	File Sharing	13,8 %	6,7 %
Итого:		16,84 %	8,17 %

2. Определяем количество точек доступа, требуемое для обслуживания каждого клиента. «Низкоскоростные» клиенты будут ассоциироваться с точкой доступа в диапазоне 2,4 ГГц. Для обслуживания 10 ноутбуков потребуется примерно $10 \cdot 0,3371 \approx 4$ точки доступа. «Высокоскоростные» клиенты будут ассоциироваться с точкой доступа в диапазоне 5 ГГц. Для обслуживания 30 ПК с беспроводным адаптером потребуется примерно $30 \cdot 0,0817 \approx 3$ точки доступа.

3. Определяем итоговое количество точек доступа. Поскольку для построения сети выбраны двухдиапазонные точки доступа, одновременно обслуживающие клиентов в разных диапазонах, то сначала надо вычислить суммарное количество точек доступа, требуемое для обслуживания клиентов каждого типа в каждом диапазоне. Далее значения, полученные для диапазонов 2,4 и 5 ГГц, надо сравнить и выбрать из них максимальное. В нашем случае для построения сети в диапазоне 2,4 ГГц требуется 4 точки доступа, а в диапазоне 5 ГГц — 3 точки доступа. Таким образом, для создания сети необходимо 4 двухдиапазонные точки доступа DAP-2660.

Все приведенные расчеты являются ориентировочными. В процессе проектирования они должны будут уточняться.

7.3.2. Скорость передачи данных и дальность действия беспроводной сети

Скорость передачи данных влияет не только на производительность беспроводной сети, но и на расстояние передачи. Чем выше скорость, тем меньше расстояние, на которое может быть передан сигнал (см. в 6.2). Основная причина сокращения расстояния при увеличении скорости связана с тем, что большая скорость требует большей мощности сигнала на входе прием-

ника. Производители указывают значение чувствительности в характеристиках беспроводного оборудования для конкретной скорости передачи, так как именно это определяет достижимую дальность связи для каждой конкретной скорости передачи.

Клиент сможет достичь максимальной скорости передачи в том случае, если он передает точке доступа и принимает от нее сигнал наибольшей мощности, существенно превышающей требуемую чувствительность при минимальном влиянии интерференции и препятствий на сигнал. В случае удаления клиента от точки доступа или наличия каких-то препятствий на пути сигнала точка доступа автоматически снижает скорость передачи, а при приближении клиента к точке доступа или снижении влияния препятствий или интерференции — повышает. По умолчанию скорости передачи точки доступа и клиентов устанавливаются автоматически благодаря процессу адаптивного выбора скоростей. Также автоматически будет изменяться мощность передатчика при изменении скоростей. Максимальной мощностью передатчика будет при минимальных скоростях передачи, так как сигналу требуется пройти большее расстояние или преодолеть препятствия.



Рис. 7.4. Обратная зависимость скорости и расстояния передачи

Если проект беспроводной сети нацелен на достижение максимальной производительности, клиенты должны подключаться к точкам доступа на максимально возможных скоростях, что сокращает время использования ими канала. Поскольку канал является разделяемым, то сокращение времени его использования позволяет или подключить к точке доступа дополнительных клиентов или выделить больше канального времени существующим клиентам. Зона действия точки доступа в сети, нацеленной на достижение максимальной производительности, будет меньше, чем в сети, нацеленной на достижение максимальной зоны покрытия (рис. 7.4). Поэтому если в сети используется несколько точек доступа, для обеспечения роуминга соседние точки надо располагать ближе друг к другу. Чтобы вычислить расстояние, на котором клиент сможет передавать и получать данные от точки доступа на требуемой скорости, можно воспользоваться формулами, представленными в 6.2.

7.3.3. Выбор частотного диапазона

Выбор частотного диапазона является важным этапом проектирования беспроводной сети. В настоящее время наибольшее число беспроводных сетей работает в диапазоне частот 2,4 ГГц, что связано с историей появления и развития спецификаций 802.11, 802.11b, 802.11g. Спецификация 802.11a не получила широкого распространения, так как большинство выпускаемых клиентских беспроводных устройств было оборудовано интерфейсами для работы в диапазоне 2,4 ГГц. Появление устройств 802.11n и 802.11ac дало возможность выбирать рабочий частотный диапазон. Эти устройства могут работать в диапазоне 2,4 или 5 ГГц или в обоих диапазонах одновременно. При этом сохранилась обратная совместимость с устройствами, поддерживающими спецификации 802.11a, 802.11b, 802.11g. Поэтому диапазон 2,4 ГГц уже не является безальтернативным вариантом. Прежде чем определиться с выбором рабочего частотного диапазона, необходимо рассмотреть ряд вопросов.

- Регулирование радиочастотного спектра отличается в разных странах. Использование диапазона 2,4 ГГц в целом имеет меньше ограничений по сравнению с диапазоном 5 ГГц.

- Доступная полоса пропускания. Ширина спектра в диапазоне 5 ГГц значительно больше по сравнению с шириной спектра 2,4 ГГц. В диапазоне 5 ГГц можно использовать каналы шириной 80 и 160 МГц, что значительно повышает производительность сети (при условии, что сеть построена на оборудовании 802.11ac).

- Дальность действия сети. Известно, что с увеличением частоты сигнала дальность его передачи уменьшается. Следовательно, сети, использующие диапазон 5 ГГц, должны обладать меньшей дальностью действия по сравнению с сетями диапазона 2,4 ГГц. Однако это справедливо не во всех ситуациях. Разные среды могут по-разному влиять на распространение сигналов 2,4 и 5 ГГц. Также следует учитывать сильную зашумленность диапазона 2,4 ГГц, что делает дальность действия сетей 2,4 и 5 ГГц в некоторых случаях практически одинаковой.

- Интерференция. Поскольку в диапазоне 2,4 ГГц работает большинство беспроводных сетей, а также различных бытовых приборов (микроволновые печи, радиотелефоны, устройства Bluetooth и т.п.), интерференция сигналов в диапазоне 2,4 ГГц выше, чем в диапазоне 5 ГГц. Однако с распространением устройств 802.11ac интерференция в диапазоне 5 ГГц будет постепенно возрастать.

- Имеющиеся клиентские устройства. Выбор диапазона сети будет зависеть от рабочего диапазона клиентских устройств, которые используются или будут использоваться в сети.

Если точка доступа или маршрутизатор поддерживают одновременную работу в диапазонах 2,4 и 5 ГГц, то наилучшим решением является использование сразу обоих диапазонов. Поскольку ширина спектра в диапазоне 5 ГГц значительно больше по сравнению с шириной спектра 2,4 ГГц, имеются устройства, позволяющие создавать независимые сети в разных полосах

диапазона 5 ГГц. Например, беспроводной маршрутизатор D-Link DIR-890L одновременно работает в диапазоне 2,4 ГГц, а также в нижней и верхней полосах диапазона 5 ГГц. Таким образом, он позволяет создавать три независимые WLAN: одну стандарта 802.11n в диапазоне 2,4 ГГц и две сети стандарта 802.11n или 802.11ac в диапазоне 5 ГГц (рис. 7.5).

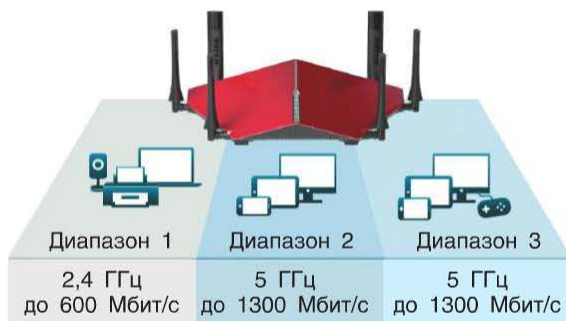


Рис. 7.5. Создание независимых беспроводных сетей с помощью D-Link DIR-890L

7.3.4. Настройка мощности передатчика

Современные точки доступа предоставляют возможность настройки мощности передатчика, которая по умолчанию установлена на максимальное значение. Установка максимальной мощности передатчика дает, с одной стороны, преимущества большого радиуса действия сети и уменьшения количества точек доступа, требуемых для обслуживания клиентов, а с другой стороны, при очень высокой плотности размещения точек доступа на какой-то территории (например, многоквартирный дом, офисное здание, корпоративная сеть с большим количеством беспроводных устройств) максимальная мощность излучения приводит к интерференции среди точек, работающих на перекрывающихся или одинаковых каналах, что будет снижать их производительность.

При проектировании беспроводной сети, нацеленной на достижение максимальной зоны обслуживания, настройка максимальной мощности излучения (рис. 7.6) вполне оправдана. Как правило, такие сети создаются на больших промышленных или складских территориях или вне помещений. В этом случае плотность размещения устройств невысока и влияние интерференции на соседние каналы будет небольшое. При проектировании сети, нацеленной на достижение максимальной производительности, мощность передатчиков точек доступа необходимо снижать. Снижение мощности передатчиков соседних точек доступа позволит повысить производительность сети за счет уменьшения интерференции в перекрывающихся и повторно используемых (одинаковых) каналах, а также повысить защищенность сети, так как слабый сигнал с большой долей вероятности не сможет распространяться за границы территории, на которой расположена сеть.

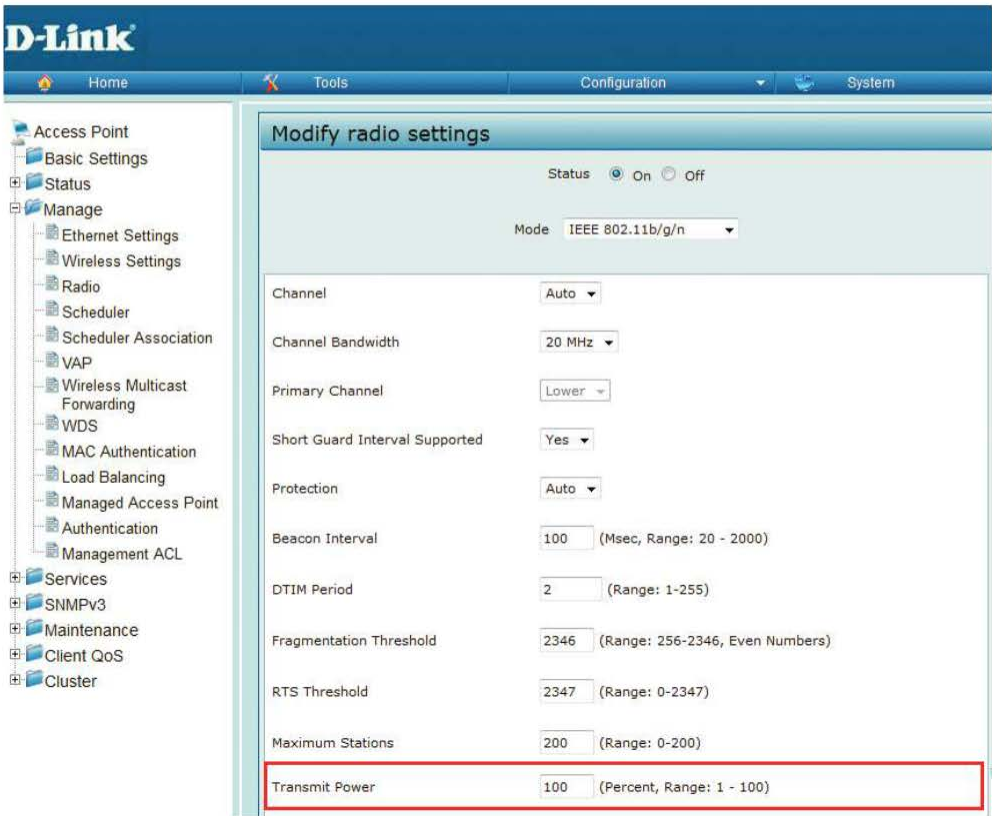


Рис. 7.6. Настройка мощности передатчика

7.3.5. Использование антенн

Антенны, с которыми поставляются точки доступа, обычно имеют коэффициент усиления от 2 до 5 dBi, всенаправленную диаграмму направленности и конструктивно бывают съемными и несъемными. Если на точке доступа со съемной антенной поменять штатную антенну на всенаправленную или направленную антенну с высоким коэффициентом усиления, то расстояние передачи сигналов увеличится как от точки доступа к клиенту, так и от клиента к точке доступа.

Напомним, что передачи в беспроводных сетях двухсторонние и характеристики линии связи от точки доступа к клиенту и от клиента к точке доступа могут не совпадать. В отличие от повышения выходной мощности передатчика, которое влияет на увеличение расстояния передачи только в одну сторону, использование антенны с высоким коэффициентом усиления улучшает и передачу, и прием радиоволн (рис. 7.7).

Использование направленных антенн позволяет решать проблемы, возникающие при необходимости покрытия нестандартных областей внутри или

вне помещений, наличии ограничений по монтажу точек доступа, а также при повторном использовании каналов большим количеством точек доступа сети. При правильной ориентации направленные антенны позволяют создавать зоны действия небольшого размера, что повышает безопасность сети и способствует изоляции ячеек, работающих на одинаковых каналах.

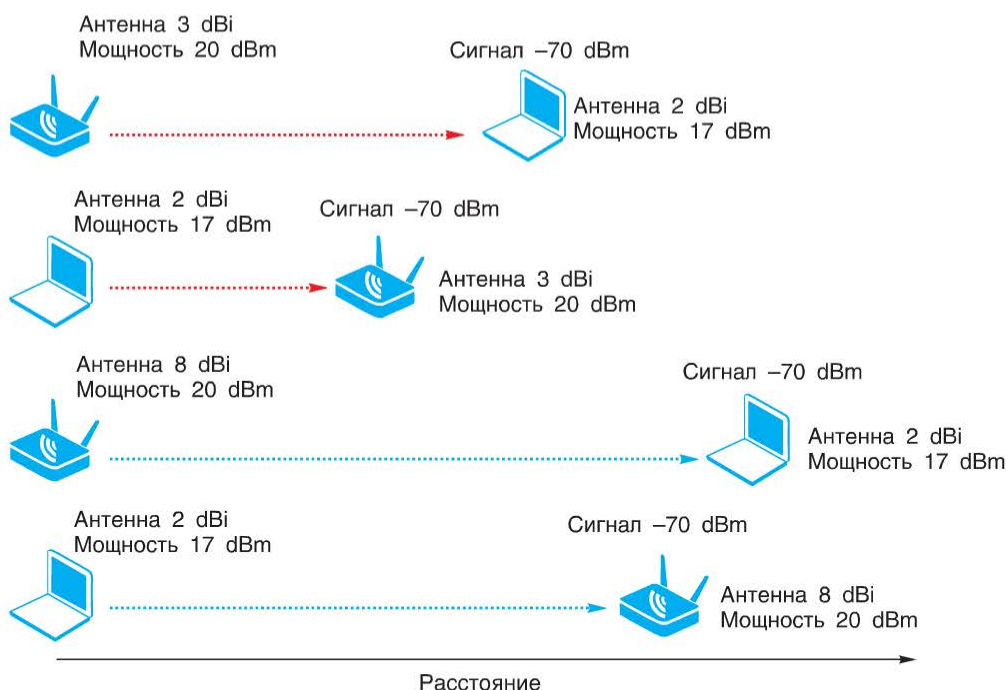


Рис. 7.7. Зависимость расстояния от мощности и коэффициента усиления антенны

Напомним, что по типу исполнения антенны делятся на комнатные (для использования внутри помещений) и уличные (вне помещений).

Внимание: выходная мощность передатчика и эквивалентная (эффективная) изотропно-излучаемая мощность (ЭИИМ) радиоэлектронных устройств регулируются государственными органами. Основные технические характеристики и условия использования устройств Wi-Fi внутри и вне закрытых помещений в полосах радиочастот 2400–2483,5 МГц, 5150–5350 МГц и 5650–5850 МГц регламентируются Решениями ГКРЧ.

7.3.6. Выбор радиочастотного канала

При использовании одной точки доступа в домашней сети или сети небольшого офиса не возникает проблем, связанных с радиочастотным планированием: ее можно настроить на работу на любом канале. По умолчанию

на большинстве точек доступа выполняется автоматический выбор рабочего канала, который обеспечивает наилучшую производительность в зависимости от условий зашумленности окружающей среды. Многие домашние пользователи или пользователи в небольших компаниях при установке устройства не изменяют настроек по умолчанию. В результате на каналах по умолчанию может быть настроено множество точек доступа многоквартирного дома или офисного здания, что приводит к негативному влиянию соседних точек доступа друг на друга.

Посмотреть загруженность каналов можно с помощью любой программы мониторинга беспроводной сети (рис. 7.8).

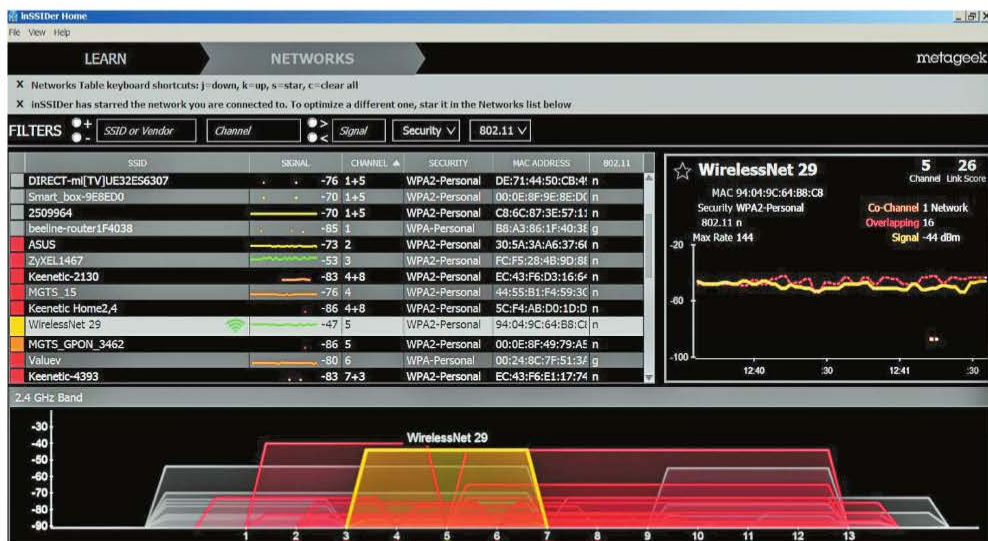


Рис. 7.8. Информация о каналах и сетях в программе мониторинга inSSIDer

Настройки канала точки доступа можно вручную изменить через интерфейс администрирования устройства (рис. 7.9). Рекомендуется настраивать точку доступа на один из неперекрывающихся каналов во избежание интерференции.

Настройка множества соседних точек доступа домашней сети на один и тот же канал не сильно скажется на производительности, поскольку в таких условиях использование сети обычно невысокое. К выбору частотного плана средних и больших корпоративных беспроводных сетей с использованием множества точек доступа и передач большого объема трафика надо подходить более внимательно.

Настройка каналов по умолчанию в этом случае является не лучшим решением. Для обеспечения мобильности клиентов (роуминга) зоны действия точек доступа пересекаются. Если все точки доступа будут настроены на работу в одном канале, возникает *межканальная интерференция (co-channel*

interference, CCI) (рис. 7.10), в результате которой передачи в зоне действия одной точки доступа будут влиять на передачи в зоне действия другой, поскольку устройства разделяют общий канал и борются за доступ к нему (рис 7.11).

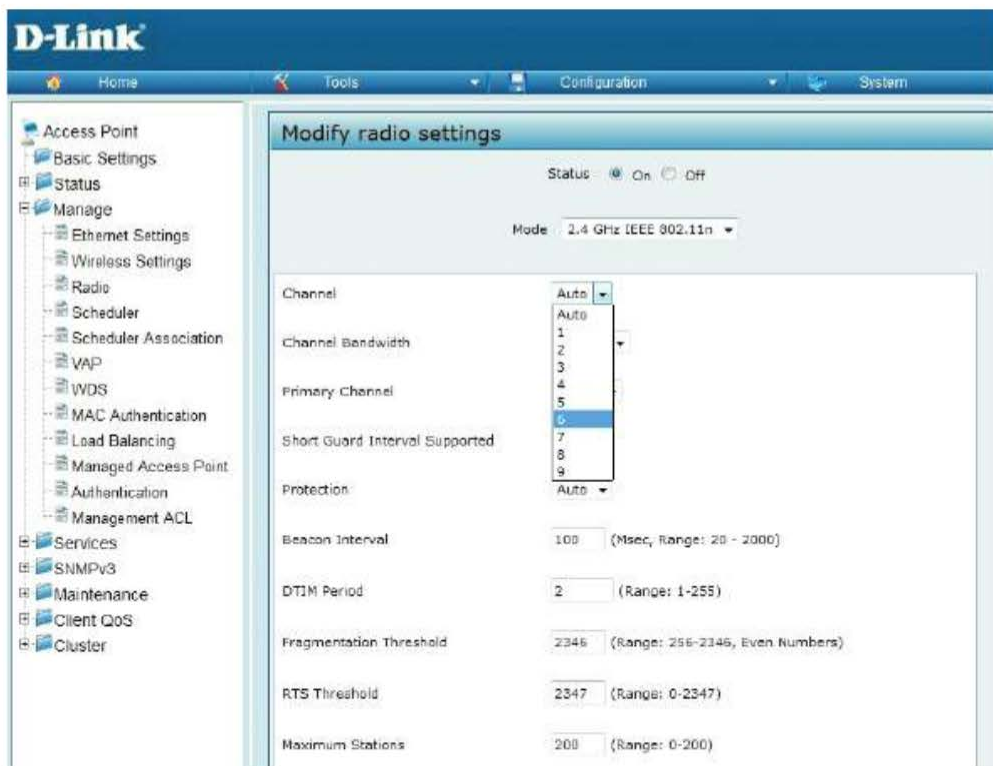


Рис. 7.9. Настройка канала на точке доступа

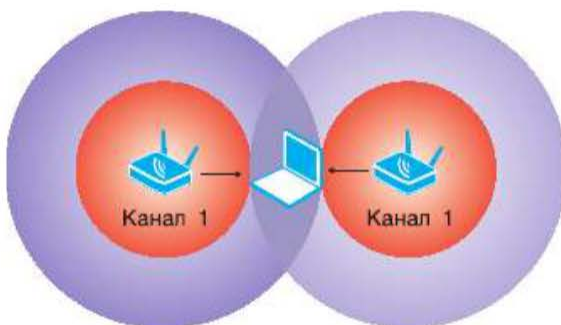


Рис. 7.10. Межканальная интерференция



Рис. 7.11. Визуализация межканальной интерференции в программе мониторинга беспроводных сетей inSSIDer

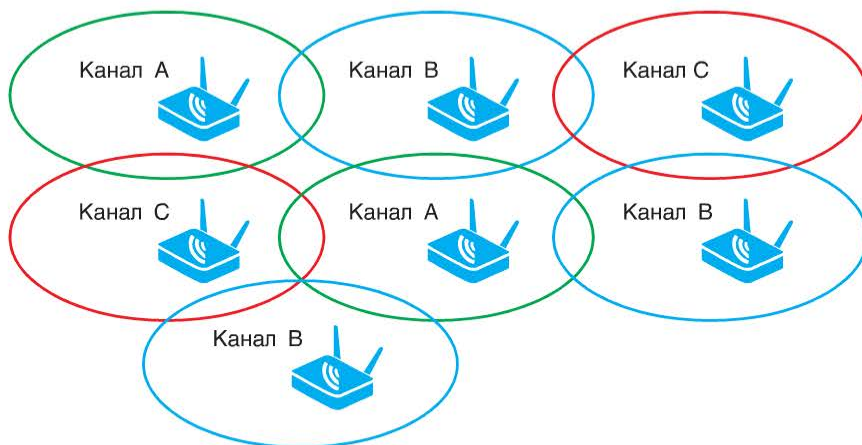


Рис. 7.12. Назначение неперекрывающихся каналов

Это приводит к ошибкам или откладыванию передачи во избежание повреждения кадров при одновременной передаче в соседней BSS. Таким образом, межканальная интерференция значительно снижает общую производительность сети. Не стоит забывать при этом, что клиентские устройства также могут создавать межканальную интерференцию. Чтобы избежать этого, соседние точки доступа настраивают на неперекрывающиеся каналы (рис. 7.12), ширина и количество которых зависит от спецификации 802.11 и радиочастотного регулирования в стране. В России в диапазоне 2400–2483,5 МГц доступно до 13 каналов (при ширине 20 МГц), три из которых являются неперекрывающимися (1, 6 и 11). Диапазон 5 ГГц не является непрерывным и включает две полосы 5150–5350 МГц и 5650–6425 МГц. Всего в частотном диапазоне 5 ГГц имеется более 20 неперекрывающихся каналов (при ширине 20 МГц), работа на которых возможна без взаимных помех. Стоит отметить, что доступное для использования количество каналов в диапазоне 5 ГГц

зависит от технических характеристик устройств. Устройство может поддерживать только нижнюю полосу 5 ГГц или верхняя полоса будет значительно уже выделенной государством для использования.

Внимание: прежде чем приступить к планированию каналов, ознакомьтесь с характеристиками беспроводных устройств и законодательными актами, регулирующими использование радиочастотного спектра.

Количество неперекрывающихся каналов ограничено, особенно в диапазоне 2,4 ГГц. Использование каналов, ширина которых больше 20 МГц, еще больше сокращает их количество. Таким образом, можно дать общую рекомендацию: в диапазоне 2,4 ГГц использовать только каналы шириной 20 МГц, в диапазоне 5 ГГц — каналы шириной 20 или 40 МГц.

В этом случае возникает вопрос планирования каналов при наличии в сети оборудования 802.11ac. Использование устройств 802.11ac в сети выглядит очень привлекательным, так как они предлагают бóльшую по сравнению с устройствами предыдущих спецификаций скорость, которая достигается благодаря использованию каналов шириной 80, 80+80 и 160 МГц.

Напомним правила выбора каналов в 802.11ac. Если точка доступа начинает работать на канале шириной 20 МГц, то этот канал не должен перекрываться с вторичными каналами 20 или 40 МГц любых соседних сетей, работающих на каналах шириной 40, 80, 160 или 80+80 МГц. Если точка доступа, использующая канал шириной 40, 80, 160 или 80+80 МГц, определяет, что существуют сети, первичные каналы 20 МГц которых перекрываются с ее вторичным каналом 20 МГц, то она должна переключиться на работу в канале шириной 20 МГц и/или изменить номер канала. При выборе первичного канала точка доступа, работающая на канале шириной 40, 80, 160 или 80+80 МГц, должна убедиться, что он не перекрывается с вторичным каналом 20 МГц соседних сетей с каналами 40, 80, 160 или 80+80 МГц и/или вторичным каналом 40 МГц сетей с каналами 160 или 80+80 МГц. Если окажется, что точка доступа занимает несколько или все каналы любых соседних сетей, то она должна выбрать первичный канал так, чтобы он совпадал с первичным каналом любой из соседних сетей.

Благодаря расширенным возможностям функции *clear channel assessment* (ССА) во вторичном канале и механизму работы с динамической полосой пропускания 802.11ac допускает наличие перекрывающихся каналов. Однако администраторы сетей должны разрабатывать частотный план так, чтобы перекрытие каналов 80 МГц было минимальным.

Рассмотрим пример, показывающий, как можно добиться минимального перекрытия каналов в сети с четырьмя точками доступа 802.11ac (рис. 7.13). Точки доступа имеют следующие характеристики: рабочая полоса частот — 5150–5350 МГц, режим работы — смешанный 802.11a, 802.11n, 802.11ac, ширина канала — 20/40/80 МГц.

Пусть на точке доступа 1 (ТД 1) в качестве первичного выбран канал 40. Точка доступа будет использовать канал 40 при передаче в канале шириной

20 МГц; каналы 36 и 40 при передаче в канале шириной 40 МГц; каналы с 36 по 48 при передаче в канале шириной 80 МГц.

Выбор канала для точки доступа 2 (ТД 2) не составляет труда, поскольку имеются незанятые каналы с 52 по 64. Канал 60 выбирается в качестве первичного канала. Точка доступа будет использовать канал 60 при передаче в канале шириной 20 МГц; каналы 60 и 64 при передаче в канале шириной 40 МГц; каналы с 52 по 64 при передаче в канале шириной 80 МГц.

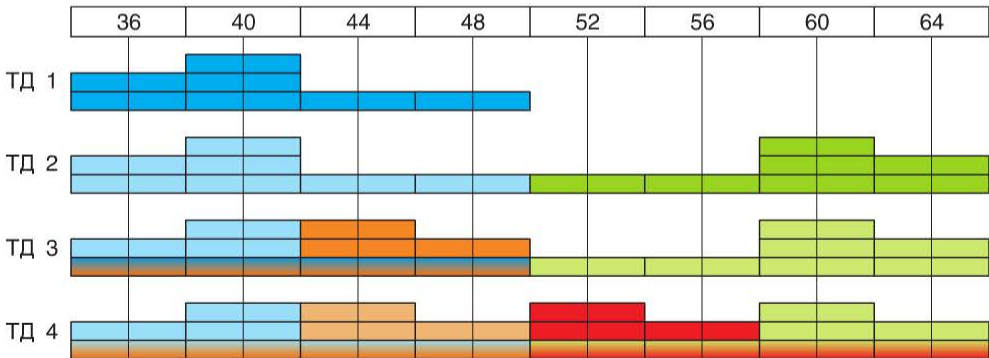


Рис. 7.13. Пример планирования каналов 802.11ac

Выбор канала для третьей точки (ТД 3) доступа уже вызывает проблемы, так как свободных каналов шириной 80 МГц не осталось. Поэтому первичный канал надо выбрать так, чтобы интерференция была минимальной. В соответствии с правилами выбора каналов первичный канал третьей точки доступа не должен перекрываться с вторичными каналами 20 МГц соседних точек. Поэтому в качестве первичного канала выберем канал 44. Таким образом, точка доступа будет использовать канал 44 при передаче в канале шириной 20 МГц; каналы 44 и 48 при передаче в канале шириной 40 МГц; каналы с 36 по 48 при передаче в канале шириной 80 МГц. Как мы видим, у точек доступа 1 и 3 каналы шириной 80 МГц полностью перекрываются, но первичные каналы 20 МГц находятся в разных каналах шириной 40 МГц. Такой выбор каналов позволяет клиентам 802.11a или 802.11n, ассоциированным с первой и с третьей точками доступа, параллельно передавать данные в каналах шириной 20 или 40 МГц. Клиенты 802.11ac, поддерживающие работу с динамической полосой пропускания, смогут воспользоваться преимуществами высокоскоростной передачи в канале 80 МГц, когда он окажется полностью свободен.

Логика выбора первичного канала для четвертой точки доступа аналогична выбору канала для третьей. В качестве первичного канала точки доступа 4 (ТД 4) выберем канал 52. Он не перекрывается с вторичными каналами 20 МГц соседних точек. Таким образом, точка доступа будет использовать канал 52 при передаче в канале шириной 20 МГц; каналы 52 и 56 при передаче в канале шириной 40 МГц; каналы с 52 по 64 при передаче в канале шириной 80 МГц.

Если потребуется добавить пятую точку доступа, то уже невозможно найти свободные каналы 80 и 40 МГц. Поэтому выбирается незанятый канал 20 МГц, например, можно выбрать канал 48 в качестве первичного канала. Канал 40 МГц будет состоять из каналов 44 и 48; канал 80 МГц будет занимать каналы с 36 по 48.

Процесс выбора каналов показан на рис. 7.13. Каналы каждой точки доступа окрашены в соответствующий цвет. Перекрывающиеся каналы окрашены в смесь двух цветов. Прямоугольники разной длины соответствуют каналам шириной 20, 40 и 80 МГц.

Ограниченное количество неперекрывающихся каналов приводит к тому, что в сетях с большим количеством точек доступа приходится использовать их повторно. В связи с этим встает задача недопущения перекрытия зон действия точек доступа, настроенных на одинаковые каналы.

При состязании за доступ к каналу сети 802.11 используют функцию *clear channel assessment* (ССА), которая определяет текущее состояние использования среды передачи. ССА основана на оценке уровня полученного сигнала. Для OFDM-устройств минимальный уровень чувствительности, определенный в стандарте, равен -82 дБм. При получении сигнала, мощность которого равна или больше минимального уровня, функция ССА сообщает, что канал занят. Поэтому во избежание межканальной интерференции между точками доступа, работающими на одном канале, рекомендуется создавать перекрытие их зон покрытия на уровне не более -85 дБм (рис. 7.14).

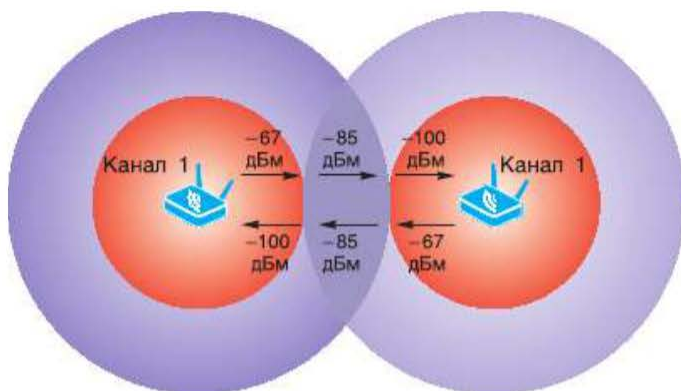


Рис. 7.14. Перекрытие зон покрытия и уровни сигналов

Перекрытие зон действия соседних точек, работающих на неперекрывающихся каналах, может быть на уровне -67 дБм, если в сети основным требованием является производительность, или на уровне -82 дБм, если сеть нацелена на обеспечение максимальной дальности действия. Общая рекомендация формулируется следующим образом: определите требования к минимальной скорости передачи сети и выполняйте перекрытие зон на соответствующем ей уровне чувствительности.

двумя способами: создать имитационную модель сети с помощью специального программного обеспечения или провести реальное обследование места ее установки.

Моделирование зоны покрытия беспроводной сети выполняется с помощью специального программного обеспечения, которое на основе исходных данных (плана помещения или карты местности, типов и материалов препятствий, высоты зданий и т. д.) производит расчет количества точек доступа, предлагает их предварительное размещение с указанием номеров каналов и визуализацией зон покрытия.

При физическом обследовании места установки беспроводной сети изучается распространение реальных радиосигналов и местоположение источников интерференции путем выполнения различных измерений и тестов. Для измерения параметров беспроводной сети проектировщику понадобятся тестовая точка доступа и тестовое клиентское устройство, на котором установлены:

- спектроанализатор, позволяющий анализировать радиочастотное окружение и обнаруживать источники помех и их физическое местоположение;
- тестер зоны покрытия, которым может быть любая программа мониторинга беспроводных сетей, позволяющая измерять мощность сигналов и шумов.

7.4.1. Моделирование зоны покрытия беспроводной сети внутри помещения

Для моделирования беспроводных сетей внутри помещений компания D-Link предлагает разработанный ею программный планировщик Wi-Fi Planner PRO. Это бесплатный инструмент проектирования, не требующий установки и доступный по адресу <http://tools.dlink.com/ru>. Для начала работы с ним требуется зарегистрироваться в системе программных инструментов D-Link.

Внимание: результатом работы планировщика Wi-Fi Planner Pro является имитационная модель беспроводной сети.

Планировщик не может использоваться для проектирования беспроводных сетей за пределами помещения или в помещении с различной высотой потолков.

Проектирование беспроводных сетей не выполняется корректно при установке точки доступа на крыше здания с высокими потолками, например склада или зала общественного назначения.

Планировщик создает имитационную модель беспроводной сети на основе следующих исходных данных: плана помещения, типа препятствий, наличия «мертвых зон», технических характеристик точек доступа D-Link, диаграмм направленности антенн и других факторов. Результатом работы проектировщика является отчет, содержащий информацию о моделях точек доступа, их количестве, местах их установки, частотном плане и карты радиопокрытия в диапазонах 2,4 и/или 5 ГГц.

Рассмотрим пример использования планировщика Wi-Fi Planner PRO для моделирования сети. До начала работы с ним в любом графическом редакторе необходимо создать план помещения, где будет установлена сеть.

Шаг 1. Создаем проект и загружаем план помещения.

Нажать на кнопку *Create project* и в открывшемся диалоговом окне ввести имя проекта (рис. 7.16).

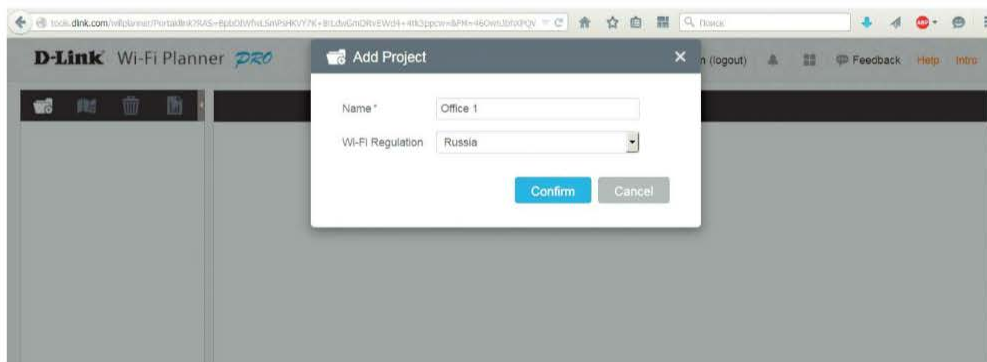


Рис. 7.16. Создание проекта

После создания проекта появится область *Add Floorplan*, при нажатии на которую откроется диалоговое окно. В поле *Name* окна необходимо ввести имя плана помещения, который можно загрузить с помощью кнопки *Browse* (рис. 7.17).

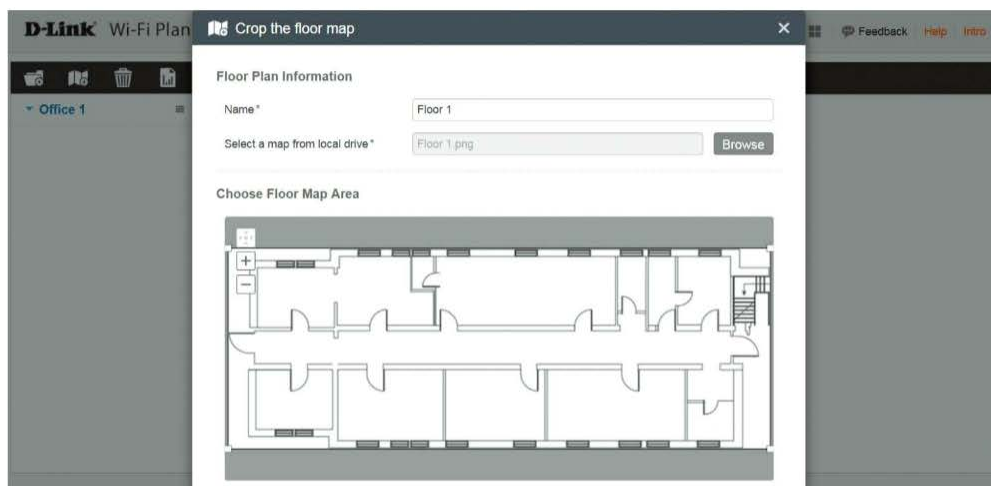


Рис. 7.17. Загрузка плана помещения

Шаг 2. С помощью инструмента *Scale* устанавливаем масштаб изображения помещения (рис. 7.18).

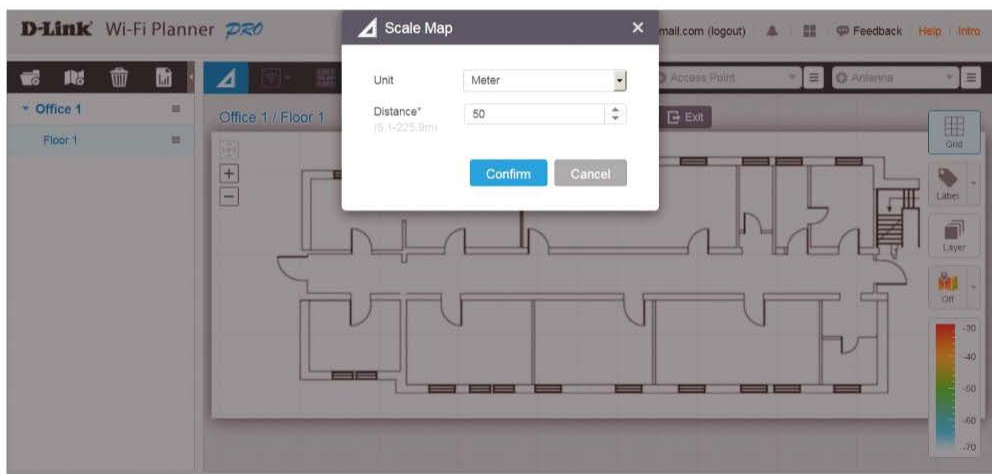


Рис. 7.18. Установка масштаба изображения помещения

Шаг 3. Определяем зону покрытия беспроводной сети (*Coverage Zone*) и зону, в которой точки доступа не будут установлены (*AP Exclusion Zone*) (рис. 7.19).

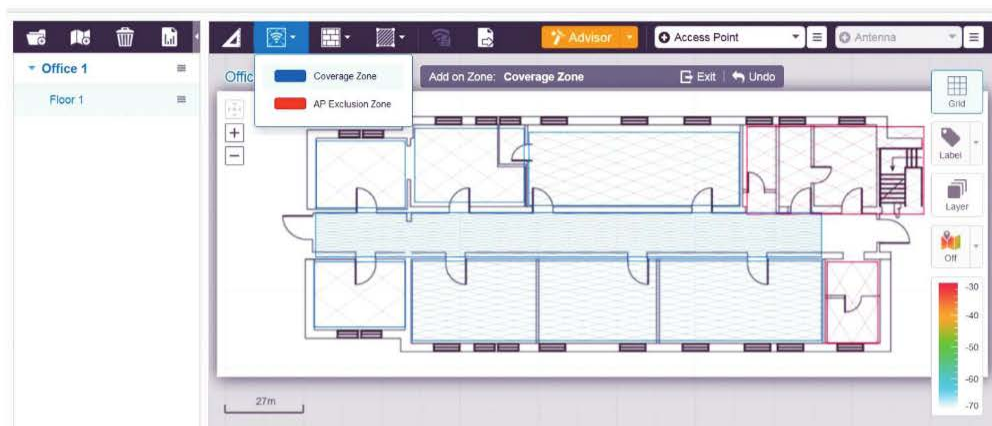


Рис. 7.19. Определение зон

Шаг 4. На плане помещения с помощью инструментов *Add obstacles* и *Add areas* указываем окна, стены, двери и особые зоны, например изолированное офисное пространство или складское помещение (рис. 7.20).

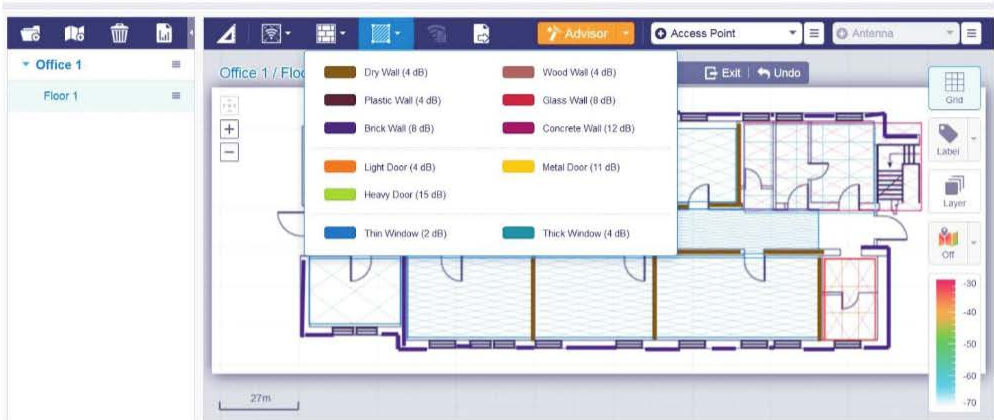


Рис. 7.20. Обозначение окон, стен, дверей и особых зон на плане помещения

Шаг 5. Запускаем мастер размещения *Advisor* для определения оптимального количества точек доступа и подходящего места их расположения. В открывшемся окне выбираем модель точки доступа, указываем процент покрытия, определяем рабочий диапазон частот, выходную мощность передатчика и минимальный уровень сигнала. Процесс размещения точек начнется после нажатия кнопки *Auto-Placement* (рис. 7.21).

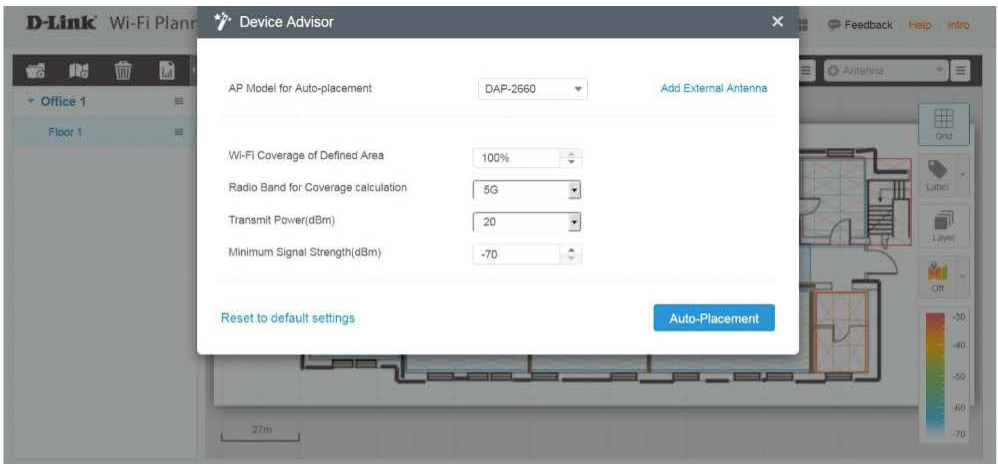


Рис. 7.21. Ввод информации для расчета размещения точек доступа

Шаг 6. После завершения расчета на плане будут показаны места установки точек доступа и их количество, назначенные каналы, а также цветовая карта, демонстрирующая теоретическую карту покрытия беспроводной сети (рис. 7.22). Цветовая карта показывает уровень сигнала на разных расстояниях от точек доступа в соответствующем диапазоне частот.



Рис. 7.22. Карта покрытия беспроводной сети

Шаг 7. С помощью инструмента *Access point list* можно посмотреть список точек доступа и их характеристики (рис. 7.23). При необходимости можно изменить рабочий частотный диапазон точек доступа и мощность передатчика.

Inventory-Access Points Inventory								
1-9 of 9								
Search								
AP Name	Model	Radio Band	Protocol	Channel	Power	Antenna Gain	Ext. Antenna(gain)	Location
AP-1	DAP-2660	2.4G On	802.11 b/g/n	1	26dBm	3	-	
AP-2	DAP-2660	2.4G On	802.11 b/g/n	11	26dBm	3	-	
AP-3	DAP-2660	2.4G On	802.11 b/g/n	6	26dBm	3	-	
AP-4	DAP-2660	2.4G On	802.11 b/g/n	11	26dBm	3	-	
AP-5	DAP-2660	2.4G On	802.11 b/g/n	1	26dBm	3	-	
AP-6	DAP-2660	2.4G On	802.11 b/g/n	1	26dBm	3	-	
AP-7	DAP-2660	2.4G On	802.11 b/g/n	6	26dBm	3	-	
AP-8	DAP-2660	2.4G On	802.11 b/g/n	6	26dBm	3	-	
AP-9	DAP-2660	2.4G On	802.11 b/g/n	11	26dBm	3	-	

Рис. 7.23. Просмотр списка точек доступа

Шаг 8. При необходимости можно внести изменения в предложенную карту покрытия. Добавить новую точку доступа можно с помощью инструмента *Access Point* (рис. 7.24). Внешнюю антенну к точке доступа, предварительно выделив ее на карте, можно добавить с помощью инструмента *Antenna* (рис. 7.25).



Рис. 7.24. Добавление новой точки доступа



Рис. 7.25. Добавление антенны



Рис. 7.26. Обновление карты с помощью инструмента HeatMap

Project Summary- 1 Floor Plans

Floor Plan Summary

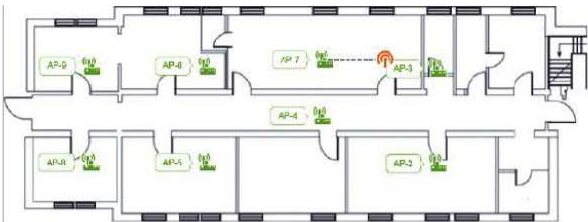
#	Name	Number of Aps	Number of Antennas
1	Floor 1	0	1
Total:		9	1

Floor Plan (Floor 1)

Floor Plan(Floor 1) : AP Inventory for Planning

AP Name	Model	Radio Band	Protocol	Channel	Power	Antenna Gain	Est. Antenna(gn to)	Location
AP-1	DAP-2660	2.4G Off	802.11 b/g/n	1	20dBm	3	-	
		5G On	802.11 a/n/ac	44	20dBm	4		
AP-2	DAP-2660	2.4G On	802.11 b/g/n	11	26dBm	3	-	
		5G On	802.11 a/n/ac	40	20dBm	4		
AP-3	DAP-2660	2.4G On	802.11 b/g/n	6	26dBm	3	-	
		5G On	802.11 a/n/ac	36	20dBm	4		

Floor Plan (Floor 1) : Map View — AP Placement



Floor Plan (Floor 1) : Map View — 2.4G HeatMap

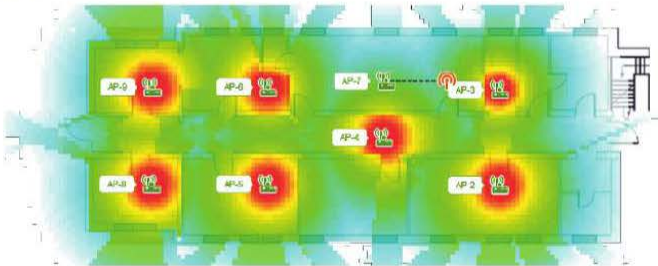


Рис. 7.27. Сформированный отчет

Также при необходимости можно изменить расположение точек доступа, «перетаскивая» их на карте, или удалить их. Заменить одну модель точки доступа на другую можно путем удаления старой точки и добавления новой.

Обновить цветовую карту после внесенных изменений можно с помощью инструмента *HeatMap*, предварительно выбрав нужный частотный диапазон (рис. 7.26).

Шаг 9. Сохранить результаты моделирования можно в виде отчета в формате PDF (рис. 7.27).

Преимуществом имитационного моделирования является возможность быстрого создания различных вариантов развертывания сети. Имитационная модель не является абсолютно точной, но она весьма удобна и эффективна как средство, облегчающее разработку сети.

7.4.2. Обследование помещения

При проектировании беспроводной сети, расположенной внутри помещения, удобно выполнять предпроектное обследование в два этапа: на первом этапе выполнить моделирование зоны покрытия, а на втором провести все необходимые измерения непосредственно на месте установки. Это позволит проверить и внести требуемые изменения в предварительный проект сети, созданный планировщиком.

Для измерения параметров беспроводной сети администратору понадобятся тестовая точка доступа и ноутбук с установленными программами мониторинга и анализа спектра.

Обследование места установки беспроводной сети начинают с его плана. Необходимо обойти помещение, отмечая на плане все препятствия, включая те, которые невозможно отобразить с помощью планировщика: шкафы, железные стеллажи, полки и т. п.; отметить все области, где будет необходима зона покрытия, а также те, где пользователи не будут подключаться к сети, чтобы сократить количество точек доступа; изучить места расположения розеток питания и Ethernet для подводки к точкам доступа питания и объединить их в BSS для обеспечения мобильности клиентов.

Наличие интерференции сильно влияет на зону покрытия точки доступа. С помощью спектроанализатора нужно определить физическое местоположение источников помех и составить список электроприборов, создающих их (микроволновые печи, мониторы, электромоторы, ИБП, радиотелефоны), а также измерить значение отношения сигнал/шум (SNR). Если оно ниже рекомендованного для большинства приложений диапазона 15–25 дБ, то удалить источники помех на максимально возможное расстояние от беспроводных клиентов и точек доступа.

Самой важной частью обследования при создании новой беспроводной сети является определение оптимального места расположения точек доступа и антенн, заменяющих штатные. При создании беспроводной сети в помещении точки доступа и антенны можно размещать на потолке, стенах, под полом.

Начинать процесс определения местоположения точек доступа следует с тестирования распространения сигналов внутри помещения. Для этого требуется настраивать тестовую точку доступа на различные режимы работы (выбирать различные каналы в диапазонах 2,4 и 5 ГГц, менять мощность передатчика) и устанавливать ее в разных точках помещения, а на клиенте с установленной программой мониторинга беспроводной сети измерять уровень сигнала (RSSI) на разных расстояниях от точки доступа. Чем большее количество мест будет использовано при измерениях, тем точнее будет результат.

Для того чтобы беспроводная сеть обеспечивала требуемый уровень производительности в любой точке зоны покрытия, необходимо определить минимальный уровень сигнала, который зависит от минимальной скорости передачи данных, определенной проектировщиком для данной сети. Надо помнить, что значение чувствительности разных моделей устройств для одной и той же скорости может отличаться. Поэтому следует изучить технические описания всех клиентских устройств и точек доступа и выбрать из всех значений чувствительности для соответствующей скорости максимальное. Это минимизирует влияние клиентов со слабыми энергетическими характеристиками на производительность сети.

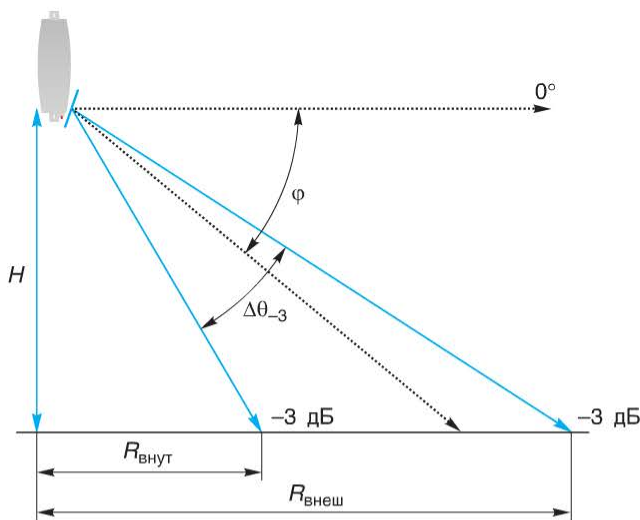


Рис. 7.28. К расчету размера зоны покрытия:

$\Delta\theta_{-3}$ — ширина главного лепестка (луча) диаграммы направленности по уровню половинной мощности (-3 дБ);
 φ — угол наклона направленной антенны к горизонту;
 H — высота расположения антенны; $R_{\text{внут}}$ — внутренний радиус зоны покрытия; $R_{\text{внеш}}$ — внешний радиус зоны покрытия

При тестировании распространения сигналов следует помнить, что для обеспечения роуминга зоны действия соседних точек доступа, работающих на неперекрывающихся каналах, должны перекрываться на уровне, который соответствует минимальной скорости передачи, определенной для данной сети. Зоны точек доступа, работающих на повторно используемых (одинаковых) каналах, должны быть расположены как можно дальше друг от друга.

При установке точек доступа на потолке их штатные всенаправленные антенны обеспечивают наилучшую зону покрытия. Не рекомендуется заменять съемные штатные антенны точек доступа с низким коэффициентом усиления на внешние антенны с высоким коэффициентом усиления, если плотность размещения устройств в сети высокая. Это приведет к расширению зон действия точек доступа и появлению межканальной интерференции.

Не во всех случаях в сетях с высокой плотностью устройств удастся использовать штатные всенаправленные антенны. Это происходит, например, если требуется обеспечить покрытие нестандартных областей внутри или вне помещений или имеются ограничения по возможности монтажа точек доступа. Решить эти проблемы позволяют направленные антенны. Использовать их также удобно в том случае, если в сети большое количество точек доступа повторно использует каналы. При правильном ориентировании направленные антенны позволяют создавать зоны действия небольшого размера и хорошо изолировать ячейки, работающие на одинаковых каналах. Изменяя угол наклона направленной антенны, можно изменять размер области покрытия (рис. 7.28).

Расчет внутреннего и внешнего радиусов зоны покрытия направленной антенны можно выполнить с помощью следующих формул:

$$R_{\text{внут}} = H \tan(90^\circ - \varphi - \frac{1}{2} \Delta\theta_{-3}),$$

$$R_{\text{внеш}} = H \tan(90^\circ - \varphi + \frac{1}{2} \Delta\theta_{-3}).$$

7.5. Постпроектное обследование и тестирование сети

После того как все оборудование беспроводной сети установлено и настроено, важным завершающим этапом является постпроектное обследование и тестирование сети: с помощью инструментов мониторинга протестировать распространение сигналов беспроводной сети. Для этого нужно обойти с ноутбуком, на котором установлена программа мониторинга, всю территорию, покрываемую сетью, контролируя уровень сигнала сети (RSSI). При необходимости изменить местоположение точек доступа и антенн, отрегулировав мощность излучения или добавив новые точки доступа.

Функции мониторинга и регистрации событий, поддерживаемые программным обеспечением точек доступа, беспроводных маршрутизаторов

и контроллеров, позволят контролировать состояние устройств и подключенных к ним клиентов, а также получать информацию о настроенных функциях, уровнях сигнала, используемых частотных диапазонах и т. д.

Следует удостовериться, что каждый клиент может ассоциироваться как минимум с одной точкой доступа. В противном случае нужно проверить его конфигурацию и конфигурацию точек доступа.

Кроме того, необходимо проверить настройку функций безопасности на клиентах, точках доступа, беспроводных маршрутизаторах и контроллерах, установленных в сети, провести тесты, проверяющие возможность подключения к сети неавторизованного клиента или точки доступа. Например, предположив, что злоумышленник знает SSID и пытается подключиться к этой сети, настроить одно из клиентских устройств с этим SSID и попытаться ассоциироваться с какой-нибудь из точек доступа. Если ассоциация произойдет, значит функции обеспечения безопасности на этой точке доступа не настроены или настроены неправильно.

8. Развертывание беспроводной сети

Архитектура беспроводной сети согласно стандарту 802.11 может рассматриваться как тип архитектуры на основе ячеек (сот), в которой каждой ячейкой (сотой) является базовый набор услуг (BSS), контролируемый точкой доступа. BSS может быть изолирован или соединен с другими BSS распределительной системой (*distribution system*). Два и более BSS с одним именем SSID, соединенные распределительной системой, называются расширенным набором услуг (ESS). Точка доступа обеспечивает подключение к распределительной системе, предоставляя ее сервисы, а также выступает в роли беспроводной станции. Еще одним логическим компонентом сетевой инфраструктуры является портал, который интегрирует архитектуру 802.11 с проводной локальной сетью.

Стандарт 802.11 не описывает детальную реализацию распределительной системы, но определяет набор услуг, позволяющих передавать кадры между двумя объектами сети (см. 2.2).

Производители самостоятельно реализуют в своем оборудовании услуги, определяемые стандартом, а также дополнительные функции, такие как балансировка нагрузки, поддержка станций сотовой связи, обнаружение несанкционированных точек доступа, наличие которых следует учитывать при развертывании беспроводной сети.

8.1. Проблемы при развертывании больших беспроводных сетей

В RFC 3990 определены четыре основные проблемы, возникающие при развертывании больших сетей WLAN:

1) каждая точка доступа требует настройки, мониторинга и контроля. В больших сетях число точек доступа обычно превышает 10, что требует от администратора значительных затрат времени на конфигурацию каждого устройства. Ошибочная конфигурация какой-либо точки доступа может привести к некорректной работе всей сети;

2) все точки доступа сети должны обладать единой конфигурацией, состоящей как из статической информации (адресация и аппаратные настройки), так и динамической информации (настройки соответствующей WLAN и параметров безопасности). В больших сетях обновление динамической конфигурационной информации требует значительного времени по сравнению с сетями меньшего размера, при этом поскольку обновление конфигурации точек доступа сети выполняется последовательно, в этот период времени беспроводная сеть будет иметь несогласованную конфигурацию;

3) из-за разделяемой и динамически изменяющейся природы беспроводной среды передачи, параметры точки доступа, контролирующие ее состояние, должны постоянно отслеживаться и оперативно изменяться с целью поддержания максимальной производительности WLAN. Этот процесс должен координироваться между всеми точками доступа сети во избежание возникновения интерференции между соседними устройствами. Отслежива-

ние и изменение параметров радиочастотных каналов вручную является трудоемкой и оперативно не реализуемой задачей;

4) требуется организация безопасного доступа к сети WLAN и предотвращение установки несанкционированных точек доступа. Обеспечение физической безопасности точки доступа — сложная задача, так как она не может находиться внутри закрытого серверного помещения или сетевого шкафа. Поскольку точки доступа находятся вне охраняемого помещения, устройство может быть похищено или злоумышленник, получив несанкционированный доступ к устройству, может поменять параметры безопасности WLAN.

Чтобы преодолеть большинство перечисленных выше проблем, производители сетевого оборудования предлагают собственные решения, позволяющие повысить эффективность управления и мониторинга WLAN. Компания D-Link предлагает следующие решения: использование встроенных в ПО точек доступа технологий AP Array и кластеризации; программное обеспечение SNMP-управления D-View; централизованное управление точками доступа с помощью программных и аппаратных беспроводных контроллеров.

8.2. Архитектуры беспроводных сетей

Для обеспечения совместимости устройств разных производителей в единой сети рабочая группа IETF CAPWAP проанализировала архитектуры беспроводных сетей и разделила их на три группы (RFC 4118) на основе характеристик распределительной системы: автономная, централизованная, распределенная архитектуры.

8.2.1. Автономная архитектура беспроводной сети

Автономная архитектура беспроводной сети (Autonomous WLAN Architecture) является традиционной, т. е. такой, в которой точка доступа реализует все сервисы 802.11, включая услуги распределения и интеграции, а также функцию портала. Другими словами, каждая точка доступа работает автономно, и для выполнения сервисов 802.11 ей не требуется подключение к другим устройствам. Такие точки доступа называют *автономными (Autonomous Access Point)*. Их настройка может выполняться как индивидуально через интерфейс администрирования, так и централизованно, например с помощью функции AP Array или программного обеспечения сетевого управления Central WiFiManager. Точки доступа могут соединяться между собой через распределительную систему, в большинстве случаев построенную на основе коммутаторов (рис. 8.1). Коммутаторы, соединяющие точки доступа, не должны ограничивать их максимальную пропускную способность. Например, при соединении точек доступа 802.11n или 802.11ac следует использовать коммутаторы с портами, работающими на скорости 1 Гбит/с.

Аутентификация клиентов в архитектуре с автономными точками доступа может выполняться как локально, так и с помощью внешнего централи-

зованного сервера аутентификации. С целью повышения безопасности в этой архитектуре должна быть реализована взаимная аутентификация между точкой доступа и коммутатором/маршрутизатором, к которому она подключается. Этого можно достичь, используя, например, аутентификацию на основе стандарта IEEE 802.1X. Критичным с точки зрения безопасности вопросом остается то, что точки доступа могут быть украдены и таким образом злоумышленник получит доступ к настройкам безопасности сети, так как администратор зачастую настраивает все устройства по единому шаблону.

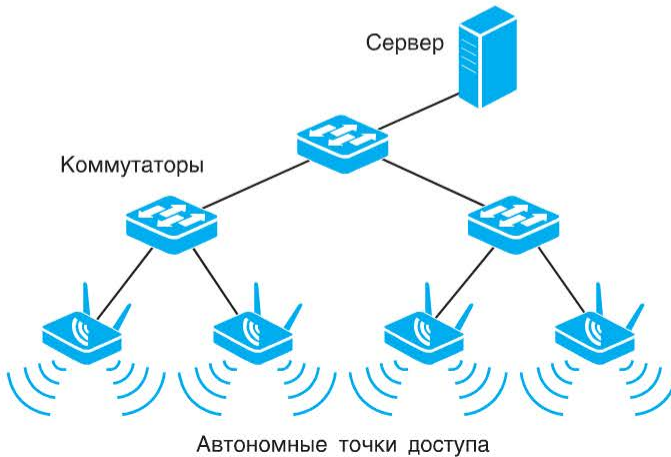


Рис. 8.1. Архитектура с автономными точками доступа

Архитектура беспроводной сети с автономными точками доступа обычно используется в домашних сетях, сетях небольших офисов, учебных классов, кафе, ресторанов, т. е. там, где требуемую зону покрытия обеспечивает не более 10 точек доступа. Увеличение количества точек доступа усложняет управление сетью. В малых сетях (домашних, офисных или сетях кафе) наилучшим решением является использование маршрутизаторов со встроенной точкой доступа, например D-Link DIR-300A, DIR-615A или DIR-620A (рис. 8.2), с помощью которых организуется беспроводной доступ, подключение к Интернету, автоматическая настройка IP-адресов, сегментация сети с помощью VLAN, контроль доступа и трафика (встроенный межсетевой экран), а также шифрование данных. При отсутствии в компании квалифицированного персонала, способного корректно настроить устройство, провайдер услуг сможет удаленно подключиться к устройству и настроить его благодаря поддержке функции клиента TR-069.



Рис. 8.2. Маршрутизаторы D-Link

8.2.2. Централизованная архитектура беспроводной сети

Централизованная архитектура беспроводной сети (Centralized WLAN Architecture) представляет собой иерархическую структуру, использующую один или более централизованных контроллеров для управления большим числом точек доступа. В отличие от автономной в централизованной архитектуре сервисы 802.11 распределены между множеством сетевых устройств, а именно точками доступа и контроллерами.

Централизованный контроллер называется *контроллером доступа (Access Controller, AC)* или *беспроводным контроллером (Wireless Controller)*. Его основной функцией является контроль и управление настройками точек доступа, присутствующих в сети. Аппаратные беспроводные контроллеры D-Link представлены двумя моделями: DWC-1000 и DWC-2000. Они поддерживают такие функции, как роуминг, управление доступом, шифрование данных, мониторинг клиентов и точек доступа, управление радиочастотными характеристиками. Функции беспроводного контроллера зачастую совмещаются с функциями коммутатора. У D-Link такие устройства получили название *беспроводных коммутаторов (Wireless Switch)* и представлены серией устройств DWS-3160-xx.

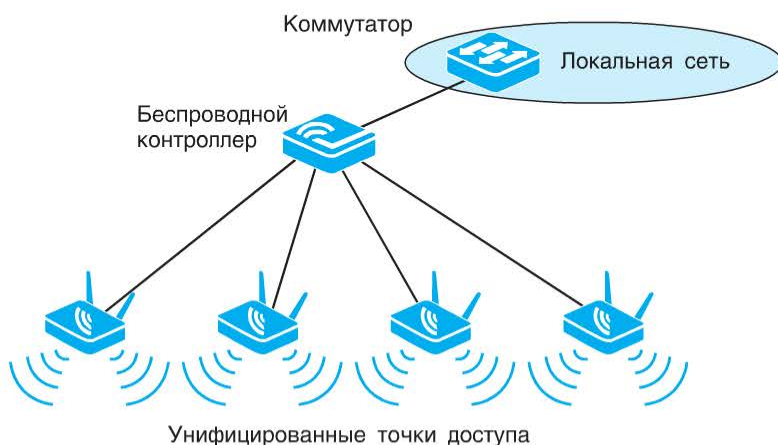


Рис. 8.3. Непосредственное подключение точек доступа к контроллеру

Существует несколько вариантов соединения беспроводного контроллера с точками доступа: непосредственное подключение (рис. 8.3), подключение через коммутатор (рис. 8.4) и подключение через маршрутизатор (рис. 8.5).

Внимание: беспроводные контроллеры и коммутаторы D-Link работают только с определенными моделями унифицированных точек доступа. Получить информацию о поддерживаемых точках доступа можно в технических описаниях устройств.

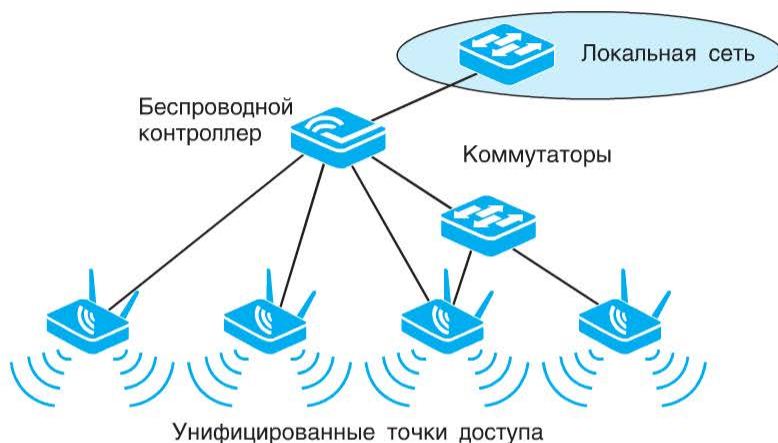


Рис. 8.4. Подключение точек доступа к контроллеру через коммутатор

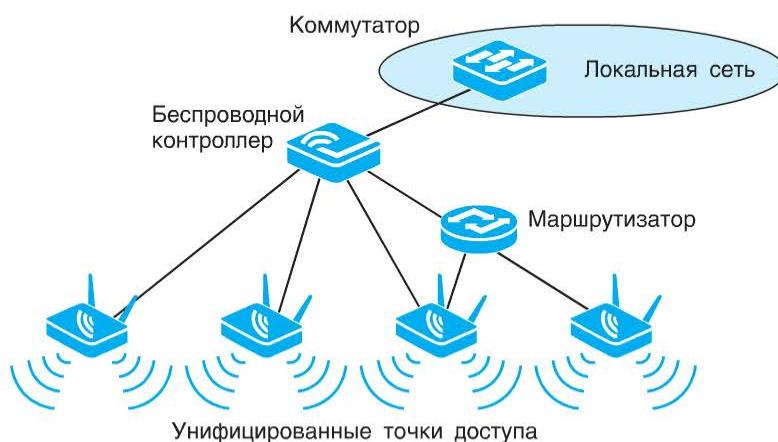


Рис. 8.5. Подключение точек доступа к контроллеру через маршрутизатор

Прежде чем начать обмениваться сообщениями, точка доступа и контроллер выполняют представленную ниже последовательность действий.

1. Обнаружение: контроллер в автоматическом режиме обнаруживает точки доступа, подключенные непосредственно к нему или через коммутатор. Администратор сети может указать точки доступа, которые будут находиться под управлением контроллера.

2. Аутентификация: контроллер проверяет подлинность точки доступа.

3. Ассоциация точки доступа с контроллером: после проверки подлинности точка доступа регистрируется на контроллере для получения управляющих и конфигурационных сообщений.

4. Установление управляющего туннеля: точка доступа устанавливает IP- или L2-туннель с контроллером для передачи данных и кадров управления.

Централизованная архитектура является наилучшим решением для сетей с количеством точек доступа, превышающим 10. При этом организация может начать построение беспроводной сети с одной унифицированной точки доступа, работающей автономно, и постепенно по мере расширения зоны покрытия и увеличения количества точек доступа перейти к централизованной архитектуре после приобретения контроллера.

Централизованная архитектура обладает следующими преимуществами при использовании в больших сетях:

1) иерархическая структура и наличие централизованного контроллера улучшают управляемость больших масштабируемых сетей. Администратор может централизованно задавать единую конфигурацию сразу для всех подключенных к контроллеру точек доступа вместо того, чтобы настраивать каждую из них в отдельности;

2) упрощается добавление в сеть новых точек доступа. Контроллер выполняет их автоматическую настройку с параметрами, аналогичными другим точкам доступа;

3) с помощью контроллера можно эффективно организовать функцию роуминга клиентов;

4) повышается общая безопасность сети, так как все точки доступа поддерживают единые настройки параметров безопасности;

5) имеется возможность организовать гостевой доступ и отделить гостевой трафик от трафика внутренней сети;

6) повышается надежность работы сети за счет поддержки функции резервирования контроллеров и механизма *AP provisioning*, позволяющего автоматически переключать управление точками доступа с вышедшего из строя контроллера на резервный;

7) повышается производительность сети за счет возможности балансировки нагрузки и регулирования параметров радиочастотных каналов на основе анализа их текущего состояния.

8.2.3. Распределенная архитектура беспроводной сети

В *распределенной архитектуре беспроводной сети (Distributed WLAN Architecture)* каждый беспроводной узел соединяется с соседними узлами через беспроводную или проводную среду передачи, формируя таким образом единую распределенную сеть. Для того чтобы обеспечить широкую зону покрытия беспроводные узлы могут работать в качестве точки доступа в их собственном BSS, а также выполнять передачу трафика через беспроводную среду другим узлам. Некоторые беспроводные узлы могут работать только в режиме передачи трафика другим узлам и не выполнять функции точки доступа для клиентских устройств. Некоторые узлы могут работать в режиме передачи беспроводного трафика и дополнительно устанавливать подключение к проводной сети, действуя в качестве портала.

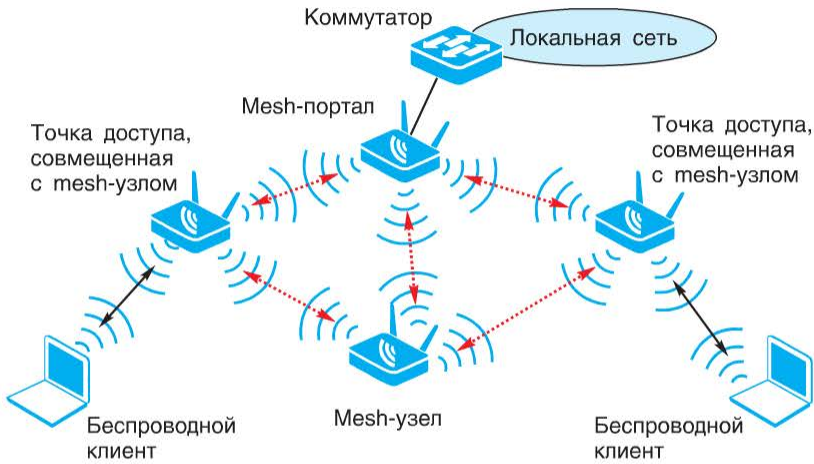


Рис. 8.6. Пример mesh-сети

Одним из примеров сети с распределенной архитектурой является *беспроводная ячеистая сеть (Wireless Local Area Mesh Network)*, в которой беспроводные mesh-станции формируют ячеистую топологию на основе множества беспроводных соединений 802.11 с соседними mesh-станциями, даже если они находятся в разных зонах покрытия (рис. 8.6). Беспроводные ячеистые сети описаны в дополнении к стандарту IEEE 802.11s, которое в настоящее время входит в IEEE 802.11-2012. Mesh-станции устанавливают друг с другом соседские отношения, выполняют взаимную аутентификацию, обеспечивают динамическое распространение ключей шифрования и определяют наилучшие маршруты передачи кадров между узлами (выполняют маршрутизацию). Протоколы, позволяющие определять маршрут между узлами mesh-сети, являются собственной разработкой производителей, поэтому использование оборудования разных производителей в единой mesh-сети невозможно. Ячеистые сети обеспечивают высокую надежность, так как mesh-станции отслеживают состояние своих соседей и в случае выхода из строя какого-либо узла динамически перестраивают маршруты. Настройка узлов mesh-сети может выполняться централизованно на контроллере.

8.3. Беспроводная распределительная система (WDS)

Традиционные точки доступа можно объединять друг с другом на основе множества беспроводных соединений 802.11 и строить таким образом распределенные сети. Это возможно в том случае, если они поддерживают функцию *беспроводной распределительной системы (Wireless Distribution System, WDS)*. Wireless Distribution System — термин, описывающий механизм соединения non mesh-станций, поддерживающих формат кадра с четырьмя полями адреса. Определение этого термина дано в стандарте IEEE 802.11-2012, но сам

механизм не является частью стандарта. Поэтому реализация WDS может отличаться в оборудовании разных производителей, в связи с чем при построении сети с WDS рекомендуется использовать устройства одного производителя.

Механизм WDS является альтернативой традиционному подходу соединения точек доступа через проводную инфраструктуру, но не исключает его. Он позволяет достичь значительной экономии средств, обеспечивает простоту настройки и добавления новых точек доступа в сеть. Управлять сетями WDS можно с помощью беспроводного контроллера, если сети построены на основе унифицированных точек доступа.

В беспроводной распределительной системе точки доступа соединяются между собой через беспроводную среду, образуя мостовые соединения. WDS предусматривает два режима работы точек доступа: режим беспроводного моста (WDS); режим беспроводного моста с функциями точки доступа (WDS with AP).

В режиме WDS точки доступа соединяются только между собой и не позволяют беспроводным клиентам подключаться к ним. В режиме WDS with AP точки доступа не только соединяются между собой, но и обслуживают подключения беспроводных клиентов (рис. 8.7).

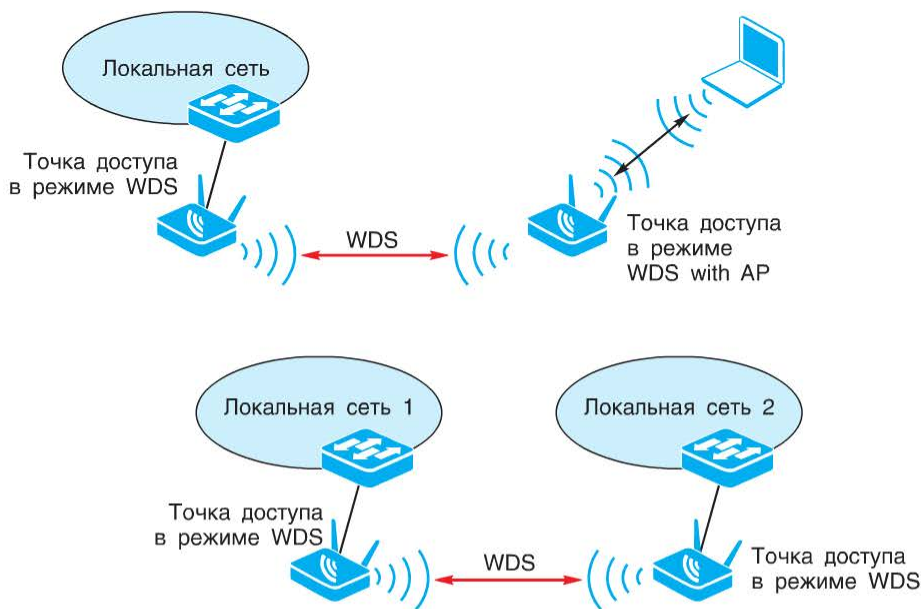


Рис. 8.7. Примеры соединений типа «точка—точка»

При работе в обоих режимах точки доступа могут устанавливать мостовые соединения типа «точка—точка» и «точка—много точек». При соединении «точка—точка» две точки доступа устанавливают между собой мостовое со-

единение. При этом каждая точка доступа может установить несколько таких соединений с разными точками доступа. Максимальное количество соединений зависит от модели точки доступа, обычно их четыре или восемь.

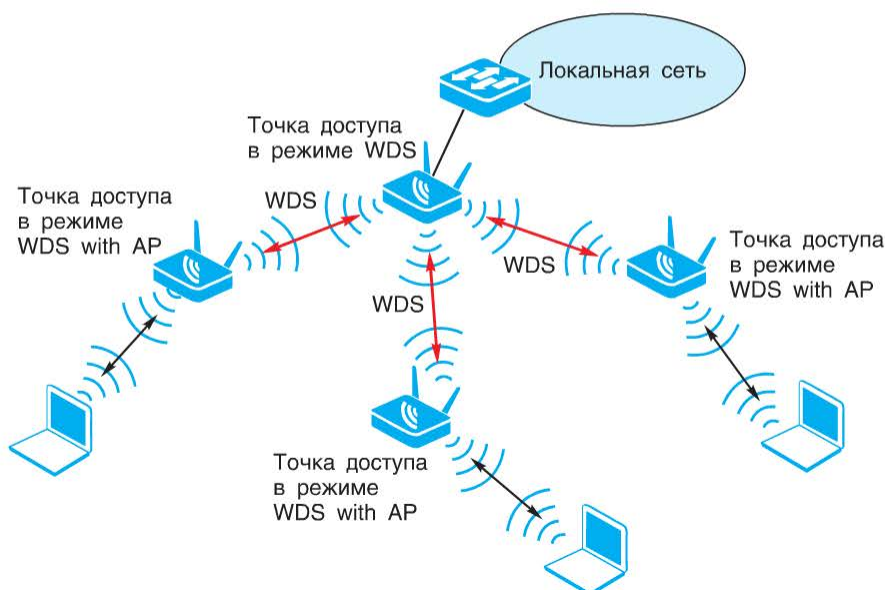


Рис. 8.8. Пример соединения типа «точка—много точек»

При соединении «точка—много точек» (рис. 8.8) точка доступа, используемая как центральная, устанавливает мостовые соединения с множеством точек доступа. Передача данных ведется через центральную точку доступа. Периферийные точки доступа друг к другу не подключаются. Максимальное количество устройств, с которыми может установить соединение центральная точка доступа, зависит от ее модели (в оборудовании D-Link — четыре или восемь точек доступа).

8.3.1. Топологии WDS-сетей

Благодаря беспроводному соединению точек доступа можно строить беспроводные сети с большой зоной покрытия, а также соединять проводные или беспроводные сетевые сегменты, расположенные как на небольшом расстоянии (в соседних зданиях или комнатах), так и на расстояниях до нескольких километров друг от друга без создания сложной инфраструктуры.

Топологии беспроводных WDS-сетей могут быть разнообразны: линейное подключение, кольцевое подключение, «звезда», ячеистая топология полной и неполной связности.

При *линейном* или *цепочечном* подключении (рис. 8.9) каждая точка доступа соединяется с предыдущей и следующей по типу «точка—точка», но

первая и последняя точки доступа в цепи не соединяются друг с другом. Добавить новую точку доступа в цепочку достаточно просто: надо указать параметры новой точки доступа в настройках последней. Для линейного подключения характерны следующие недостатки: при выходе из строя одной из промежуточных точек доступа теряется связь с сегментами сети, расположенными дальше за этой точкой. При этом несмотря на изоляцию от остальной части сети, отдельные сегменты сохраняют работоспособность.

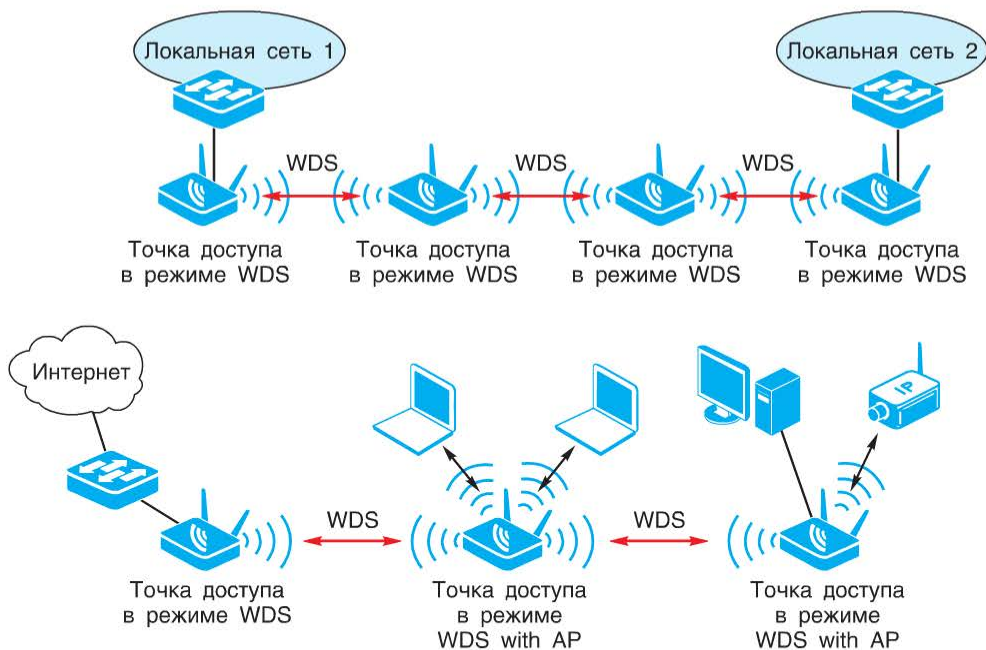


Рис. 8.9. Линейное подключение точек доступа

Кольцевое подключение (или «кольцо») получается из линейного, если соединить самую первую и самую последнюю точки доступа (рис. 8.10). При кольцевом подключении каждая точка доступа может передавать данные в любом направлении. Добавление новых точек доступа в эту топологию требует обязательной остановки работы двух крайних точек доступа, между которыми подключается новая.

Кольцевое подключение является надежным благодаря избыточным связям между устройствами. Однако следует понимать, что точки доступа не могут правильно функционировать в сетях с замкнутыми контурами. Программное обеспечение точек доступа с поддержкой WDS по умолчанию поддерживает протокол *Spanning Tree Protocol* (STP), который выявляет и блокирует лишние каналы связи между ними, а при изменении топологии сети, например из-за отключения некоторых точек или невозможности работы каналов, ранее заблокированные каналы будут использоваться взамен вышедших из строя.

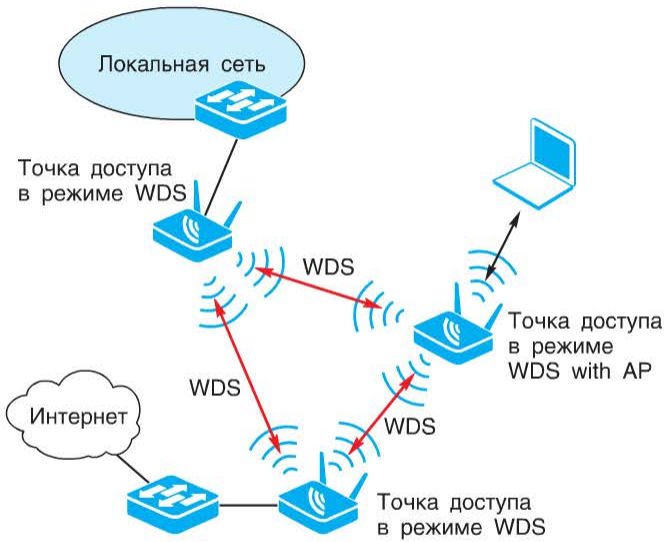


Рис. 8.10. Кольцевое подключение точек доступа

В топологии «звезда» одна точка доступа используется в качестве центральной, к которой подключаются все остальные точки (рис. 8.11). Весь обмен информацией идет исключительно через центральную точку доступа, на которую таким образом ложится значительная нагрузка.

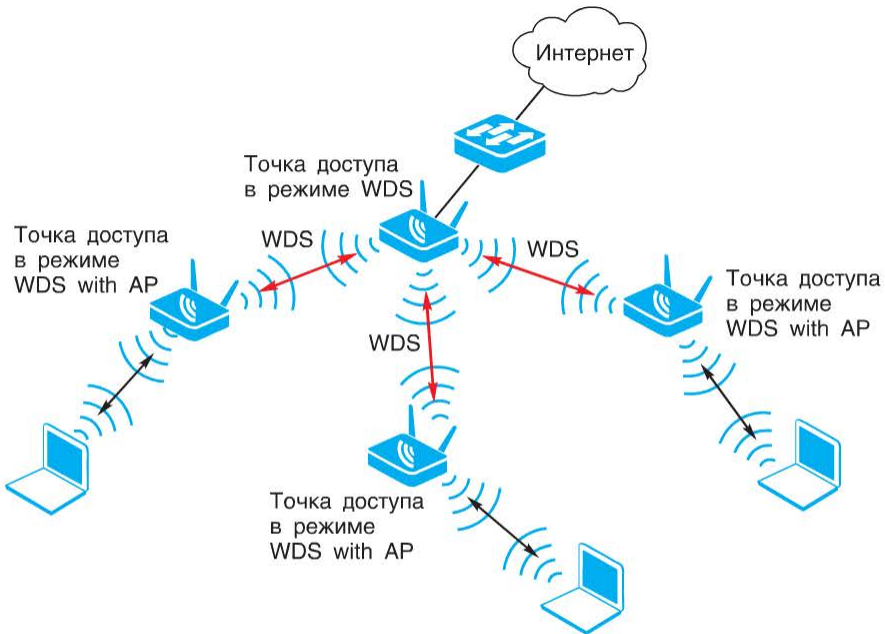


Рис. 8.11. Сеть WDS с топологией «звезда»

В качестве недостатков этой топологии можно выделить наличие единой точки отказа. Выход из строя обычной точки доступа никак не отражается на функционировании оставшейся части сети, зато отказ центральной точки делает сеть полностью неработоспособной. Еще один недостаток топологии «звезда» состоит в ограничении количества точек доступа, подключаемых к центральному устройству. Максимальное количество устройств, с которыми может установить соединение центральная точка доступа, зависит от ее модели (в оборудовании D-Link — 4 или 8 точек доступа).

В *ячеистой топологии* (mesh) каждая точка доступа соединена с множеством других каналами связи «точка—точка» (рис. 8.12). В зависимости от модели устройства максимальное количество точек доступа, с которыми оно может установить соединение, равно 4 или 8. Для корректной работы WDS-сети ячеистой топологии необходим протокол STP, устраняющий лишние связи, приводящие к заикливанию кадров.

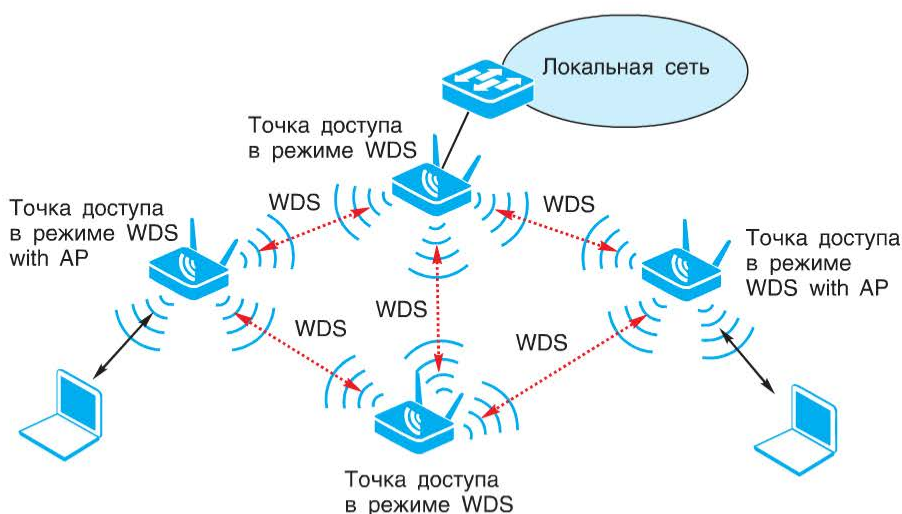


Рис. 8.12. Сеть WDS с ячеистой топологией неполной связности

Следует отметить, что при последовательном и кольцевом подключении, а также в ячеистой топологии каждая точка доступа не только принимает и обрабатывает свои данные, но и служит ретранслятором сообщений для других точек доступа. Это позволяет строить сети большой протяженности (до нескольких десятков километров).

8.3.2. Настройка WDS-соединений

Соединения WDS основываются на MAC-адресах, хранящихся точками доступа и использующими все четыре поля «Адрес» (Address 1 — Address 4) кадра. Между любой парой точек доступа может быть установлено только одно WDS-соединение, для создания которого на каждой из точек пары вруч-

ную указывается MAC-адрес соседней. При этом важно совпадение следующих настроек WDS-соединений обеих точек доступа: номер и ширина канала, SSID, алгоритмы шифрования, ключи шифрования и парольные фразы.

Важно понимать, что если точка доступа работает в режиме WDS with AP, то настройки WDS-соединения и настройки BSS не зависят друг от друга. Для того чтобы повысить общую производительность сети и избежать интерференции, рекомендуется настраивать WDS-соединения и BSS на разных частотных каналах или (если точка доступа двухдиапазонная) в разных частотных диапазонах. Поскольку одна точка доступа может установить несколько WDS-соединений с разными точками доступа, то настройки WDS-соединения между каждой парой точек доступа могут отличаться друг от друга. Другими словами, каждое соединение WDS-сети может использовать отличные от другого частотный диапазон, номер канала, SSID, алгоритмы шифрования, ключи шифрования и парольные фразы.

Примеры настройки WDS-соединений

Рассмотрим настройку WDS-соединения типа «точка—точка» между двумя двухдиапазонными точками доступа D-Link DAP-2660. WDS-соединение использует для работы диапазон 5 ГГц, клиенты подключаются к точкам доступа в диапазоне 2,4 ГГц (рис. 8.13). Настройку подключения клиентов рассматривать не будем.

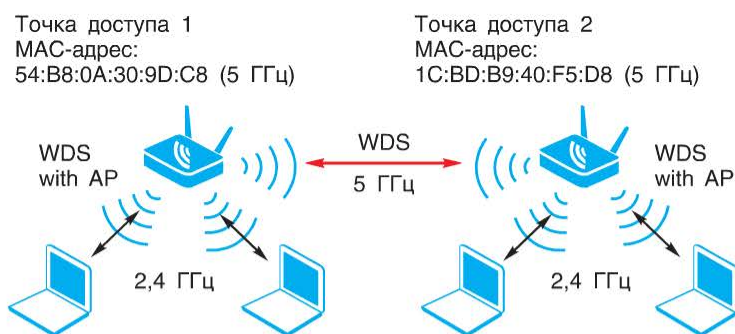


Рис. 8.13. WDS-соединение «точка—точка»

Параметры настройки WDS-соединения на обеих точках доступа должны быть одинаковыми: SSID — Dlink_TEST5, канал — 36, ширина канала — Auto 20/40 МГц, шифрование — WPA-Personal, парольная фраза 665544332211.

Порядок настройки точек доступа:

- 1) подключиться к Web-интерфейсу точки доступа;
- 2) выбрать вкладку *Basic Settings* → *Wireless*. В поле *Wireless Band* выбрать 5GHz; в поле *Mode* выбрать WDS with AP; в поле *Network Name (SSID)* ввести Dlink_TEST5; в поле *Channel* выбрать 36.

В поле *Authentication* выбрать *WPA-Personal*; в поле *PassPhrase* ввести пароль 665544332211 и повторить его в поле *Confirm PassPhrase*.

Точка доступа 1 (рис. 8.14): в окне *WDS Remote AP MAC Address* ввести MAC-адрес точки доступа 2.

Точка доступа 2 (рис. 8.15): в окне *WDS Remote AP MAC Address* ввести MAC-адрес точки доступа 1.

После выполнения всех настроек нажать кнопку *Save*;

3) проверить состояние WDS-соединения между точками доступа. Для этого зайти во вкладку *Status* → *WDS Information* на обеих точках доступа.

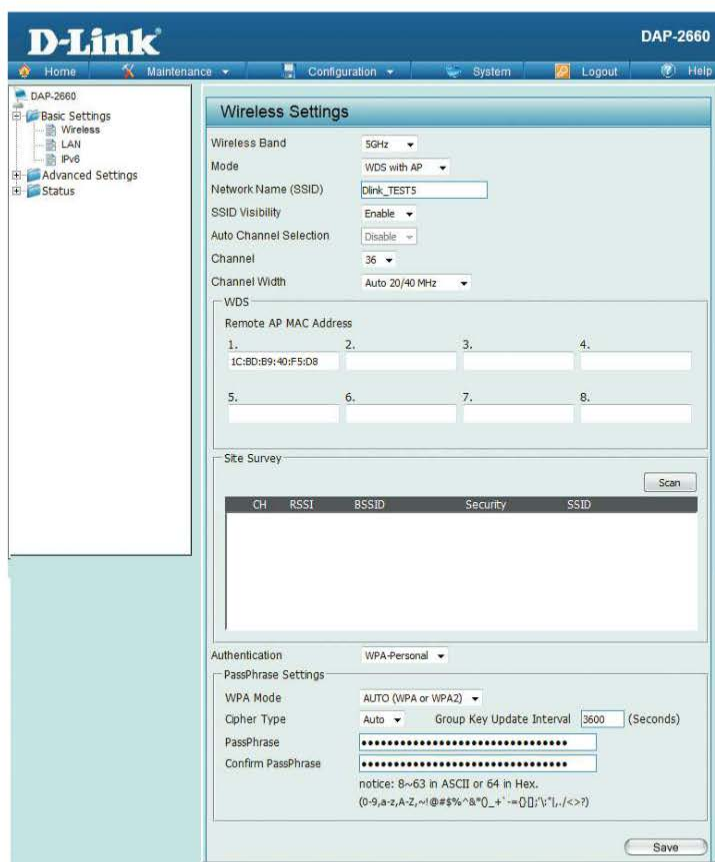


Рис. 8.14. Настройки точки доступа 1

Рассмотрим настройку WDS-сети с линейным подключением точек доступа, служащую для соединения двух сегментов локальной сети. В WDS-сети используются как однодиапазонные, так и двухдиапазонные точки доступа.

Для повышения общей производительности WDS-сети, WDS-соединения используют разные частотные каналы (рис. 8.16, табл. 8.1).

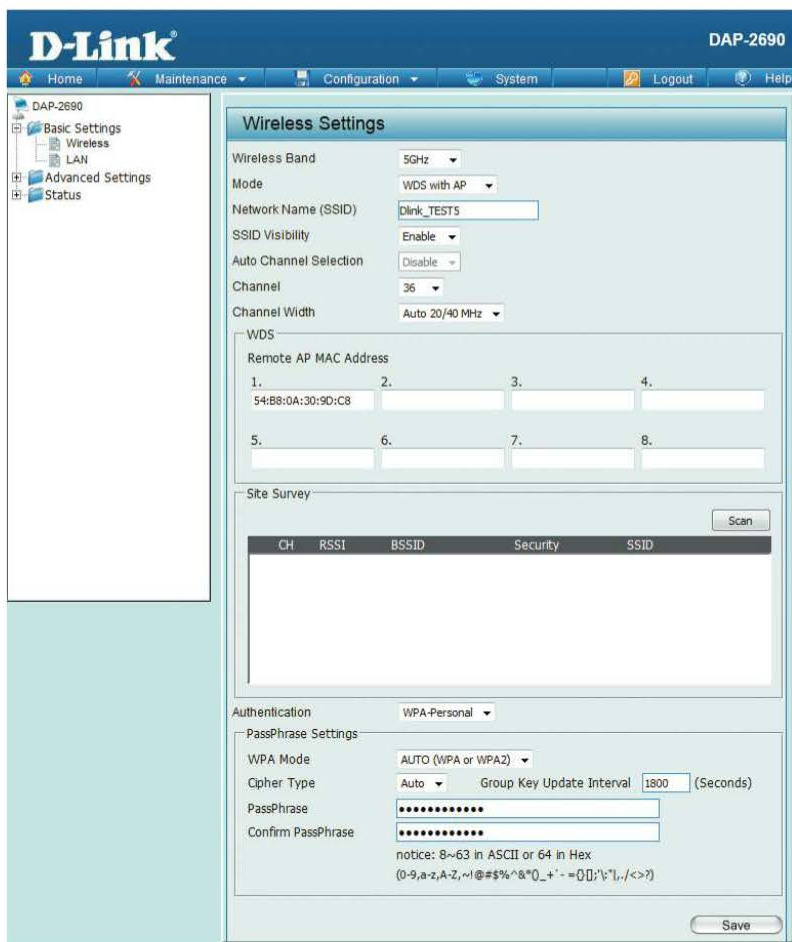


Рис. 8.15. Настройки точки доступа 2



Рис. 8.16. Соединение удаленных сегментов проводной локальной сети

Таблица 8.1. Параметры настройки WDS-соединений

Настройки WDS-соединения	
Между точками доступа 1 и 2	Между точками доступа 2 и 3
Частотный диапазон 2,4 ГГц	Частотный диапазон 5 ГГц
SSID — Dlink_TEST	SSID — Dlink_TEST5
Канал — 6	Канал — 36
Ширина канала 20 МГц	Ширина канала Auto 20/40 МГц
Шифрование — WPA-Personal, парольная фраза 112233445566	Шифрование — WPA-Personal, парольная фраза 665544332211

Настройка точки доступа 1 (рис. 8.17):
1) подключиться к Web-интерфейсу точки доступа;

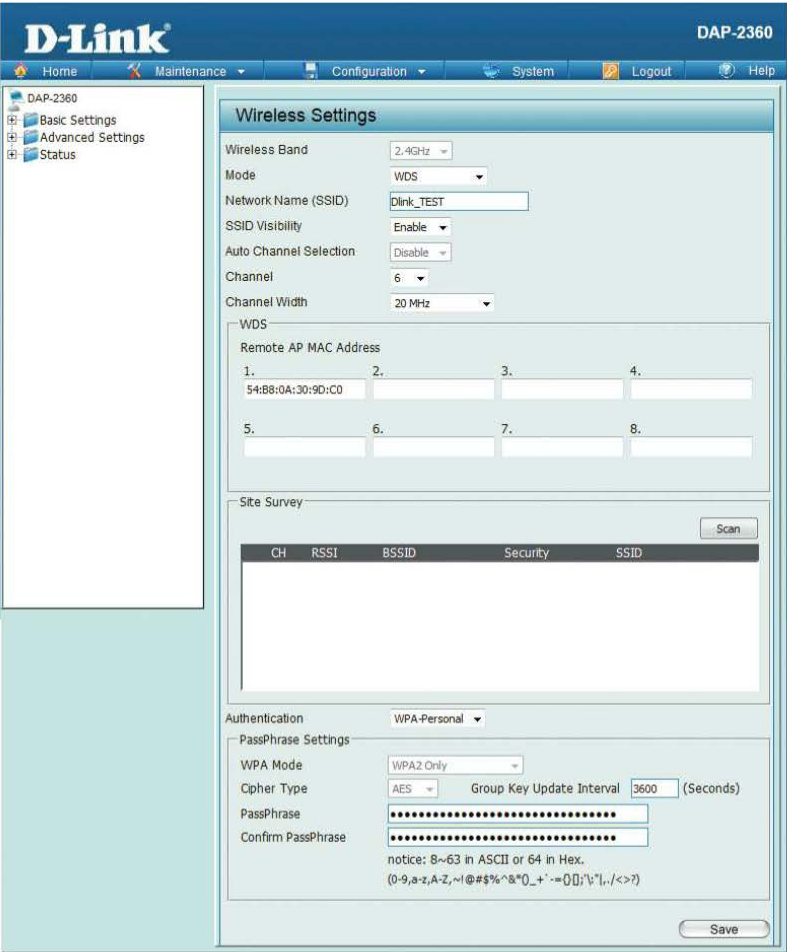


Рис. 8.17. Настройка точки доступа 1

2) выбрать вкладку *Basic Settings* → *Wireless*. В поле *Wireless Band* выбрать 2,4 GHz; в поле *Mode* выбрать WDS; в поле *Network Name (SSID)* ввести Dlink_TEST; в поле *Channel* выбрать 6; в поле *Channel Width* выбрать 20 MHz. В окне *WDS Remote AP MAC Address* ввести MAC-адрес точки доступа 2.

В поле *Authentication* выбрать *WPA-Personal*; в поле *PassPhrase* ввести пароль 112233445566 и повторить его в поле *Confirm PassPhrase*.

После выполнения всех настроек нажать кнопку *Save*.

Настройка точки доступа 2 (рис. 8.18):

1) подключиться к Web-интерфейсу точки доступа;

2) выбрать вкладку *Basic Settings* → *Wireless*. В поле *Wireless Band* выбрать 2,4 GHz; в поле *Mode* выбрать WDS; в поле *Network Name (SSID)* ввести Dlink_TEST; в поле *Channel* выбрать 6; в поле *Channel Width* выбрать 20 MHz.

D-Link DAP-2660

Home Maintenance Configuration System Logout Help

DAP-2660

- Basic Settings
- Advanced Settings
- Status

Wireless Settings

Wireless Band: 2.4GHz
 Mode: WDS
 Network Name (SSID): Dlink_TEST
 SSID Visibility: Enable
 Auto Channel Selection: Disable
 Channel: 6
 Channel Width: 20 MHz

WDS

Remote AP MAC Address

1. 54:88:0A:3A:D2:20	2.	3.	4.
5.	6.	7.	8.

Site Survey

CH	RSSI	BSSID	Security	SSID

Scan

Authentication: WPA-Personal

PassPhrase Settings

WPA Mode: WPA2 Only
 Cipher Type: AES
 Group Key Update Interval: 3600 (Seconds)
 PassPhrase:
 Confirm PassPhrase:
 notice: 8~63 in ASCII or 64 in Hex.
 (0-9,a-z,A-Z,~,!@#%&^&*0_+~=-00;'\|,./<>?)

Save

Рис. 8.18. Настройка точки доступа 2 (WDS-соединение с точкой доступа 1)

В окне *WDS Remote AP MAC Address* ввести MAC-адрес точки доступа 1. В поле *Authentication* выбрать *WPA-Personal*; в поле *PassPhrase* ввести пароль 112233445566 и повторить его в поле *Confirm PassPhrase*. После выполнения всех настроек нажать кнопку *Save*;
3) выполнить настройку WDS-соединения с точкой доступа 3 (рис. 8.19).

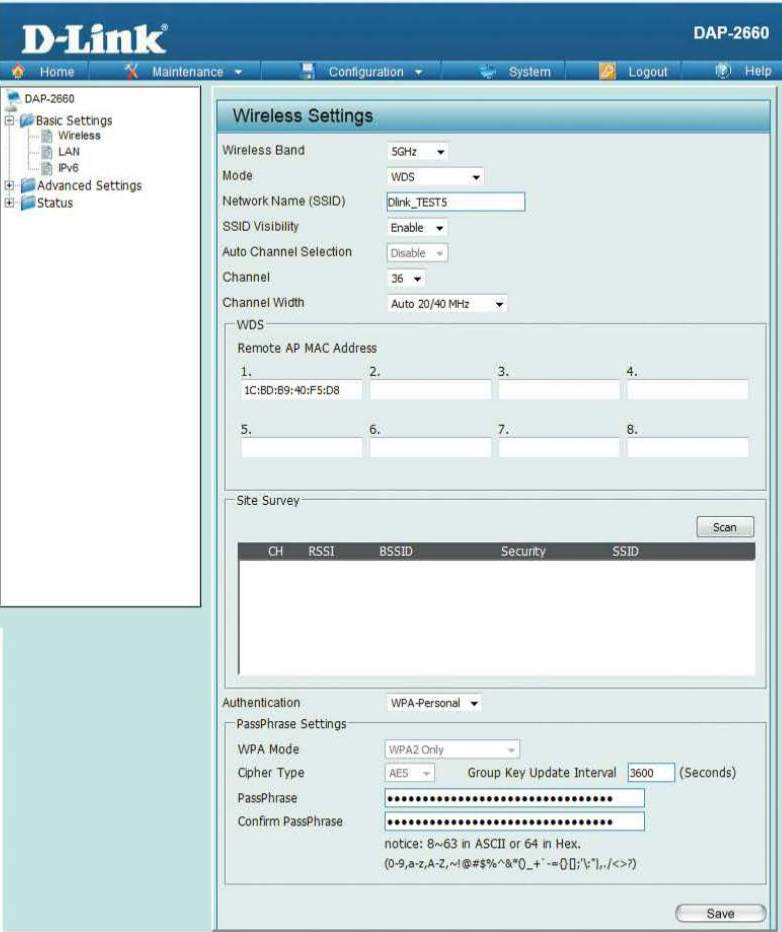


Рис. 8.19. Настройка точки доступа 2 (WDS-соединение с точкой доступа 3)

Выбрать вкладку *Basic Settings* → *Wireless*. В поле *Wireless Band* выбрать 5GHz; в поле *Mode* выбрать WDS; в поле *Network Name (SSID)* ввести Dlink_TEST5; в поле *Channel* выбрать 36. В окне *WDS Remote AP MAC Address* ввести MAC-адрес точки доступа 3. В поле *Authentication* выбрать *WPA-Personal*; в поле *PassPhrase* ввести пароль 665544332211 и повторить его в поле *Confirm PassPhrase*.

После выполнения всех настроек нажать кнопку *Save*.

Настройка точки доступа 3 (рис. 8.20):

- 1) подключиться к Web-интерфейсу точки доступа;
- 2) выбрать вкладку *Basic Settings* → *Wireless*. В поле *Wireless Band* выбрать 5GHz; в поле *Mode* выбрать WDS; в поле *Network Name (SSID)* ввести Dlink_TEST5; в поле *Channel* выбрать 36.

D-Link DAP-2690

Home Maintenance Configuration System Logout Help

DAP-2690

- Basic Settings
- Advanced Settings
- Status

Wireless Settings

Wireless Band: 5GHz
 Mode: WDS
 Network Name (SSID): Dlink_TEST5
 SSID Visibility: Enable
 Auto Channel Selection: Disable
 Channel: 36
 Channel Width: Auto 20/40 MHz

WDS

Remote AP MAC Address

1.	2.	3.	4.
54:88:0A:30:9D:C8			
5.	6.	7.	8.

Site Survey

Scan

CH	RSSI	BSSID	Security	SSID

Authentication

WPA-Personal

PassPhrase Settings

WPA Mode: WPA2 Only
 Cipher Type: AES
 Group Key Update Interval: 1800 (Seconds)
 PassPhrase:
 Confirm PassPhrase:

notice: 8~63 in ASCII or 64 in Hex
 (0-9,a-z,A-Z,~!@#\$%^&*0_+~'"/<>?)

Save

Рис. 8.20. Настройка точки доступа 3

В окне *WDS Remote AP MAC Address* ввести MAC-адрес точки доступа 2. В поле *Authentication* выбрать *WPA-Personal*; в поле *PassPhrase* ввести пароль 665544332211 и повторить его в поле *Confirm PassPhrase*.

После выполнения всех настроек нажать кнопку *Save*.

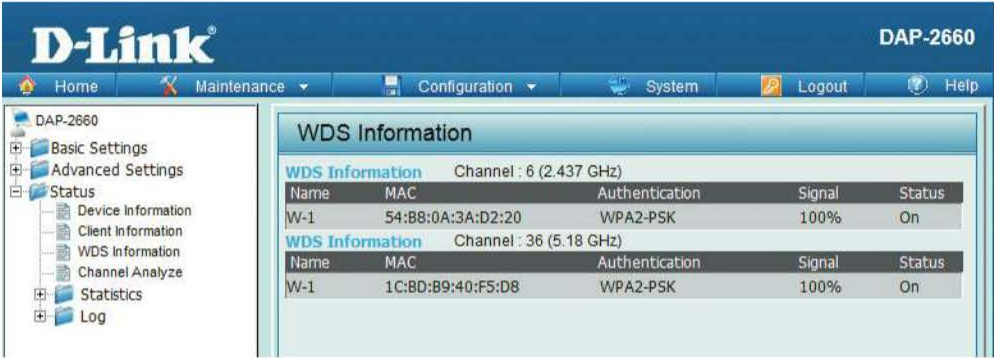


Рис. 8.21. Информация об установленных WDS-соединениях на точке доступа 2

Проверить установление соединений. Для этого на каждой из точек доступа зайти во вкладку *Status* → *WDS Information* (рис. 8.21).

8.4. Обеспечение отказоустойчивости в беспроводных сетях

При проектировании архитектуры беспроводной сети одним из важных вопросов является обеспечение ее отказоустойчивости: необходимо избежать наличия единой точки отказа и обеспечить резервирование важных архитектурных компонентов.

Используя дополнительные точки доступа, можно обеспечить резервирование беспроводных соединений. Беспроводной клиент, находящийся в любой области зоны покрытия, может подключиться к альтернативной точке доступа, если основная не предоставляет ему сервисы (например, в случае превышения лимита соединений с основной точкой доступа или если у нее возникли проблемы с программным обеспечением или радиоинтерфейсом).



Рис. 8.22. Резервирование точек доступа

Использование дополнительных точек доступа может снизить пропускную способность сети, особенно в диапазоне 2,4 ГГц, поскольку при нахождении точек доступа близко друг к другу трудно избежать их взаимной интерференции. Поэтому не рекомендуется размещать рядом основную и дополнительную точки доступа. Расстояние между ними должно быть не менее 2 м. Дополнительные точки доступа рекомендуется настраивать на работу на неперекрывающихся каналах при их наличии. Если в распределительной системе используется несколько коммутаторов, основные и дополнительные точки доступа рекомендуется подключать к разным устройствам, а в самой распределительной системе настроить функции отказоустойчивости (создать агрегированные каналы (LACP) между коммутаторами или избыточные соединения и настроить протокол STP) (рис. 8.22). Конфигурации основной и дополнительной точек доступа должны быть аналогичными.

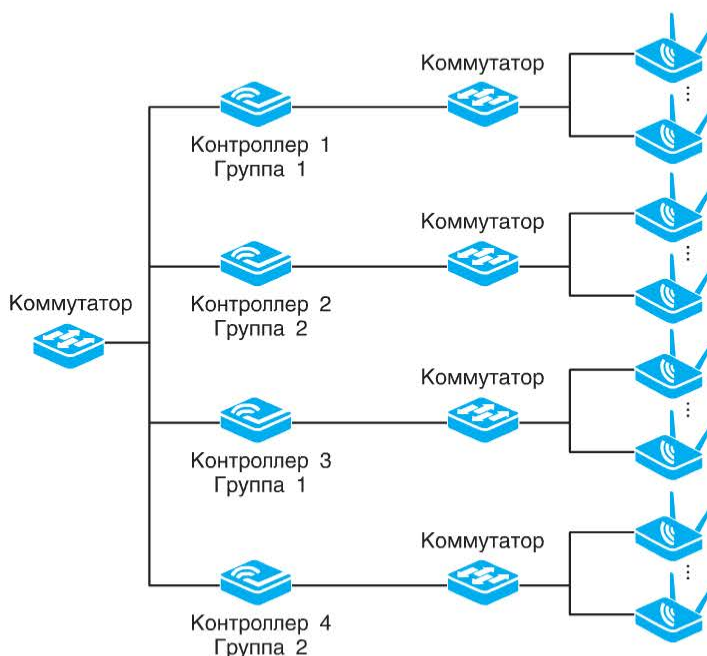


Рис. 8.23. Резервирование беспроводных контроллеров

В сетях, использующих беспроводные контроллеры, имеется больше возможностей для обеспечения отказоустойчивости по сравнению с сетями автономной архитектуры. Например, до 8 беспроводных контроллеров DWC-2000 можно объединять в кластер, внутри которого контроллеры можно разделить на группы одноранговых узлов, что позволит обеспечить их резервирование (рис. 8.23). Все контроллеры группы равноправны и обладают одинаковой информацией о подключенных к ним точках доступа. В случае выхода одного контроллера группы из строя управление обслуживаемыми им точками доступа автоматически переключается на резервный. Помимо этого в DWC-2000 реализована

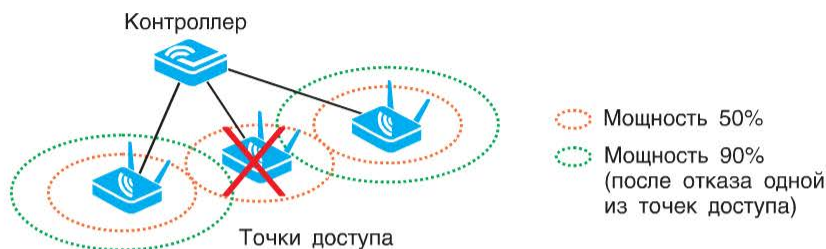


Рис. 8.24. Работа функции самовосстановления

функция самовосстановления, позволяющая при выходе из строя одной из точек доступа автоматически увеличивать мощность передатчиков соседних с целью восстановления зоны покрытия (рис. 8.24).

8.5. Режимы работы точек доступа

В программном обеспечении точек доступа может быть реализована поддержка работы в следующих режимах: Access Point; WDS with AP; WDS; Wireless Client; Repeater; Bridge. В зависимости от выбранного режима точка доступа будет выполнять в сети различные функции. Основным режимом работы точки доступа является *Access Point*. В этом режиме она выполняет свою непосредственную функцию: служит для создания беспроводной сети.

Режим беспроводного клиента (Wireless Client) (рис. 8.25) полезен в том случае, если к беспроводной сети надо подключить одно устройство, не имеющее беспроводного интерфейса и возможности для установки беспроводного адаптера.

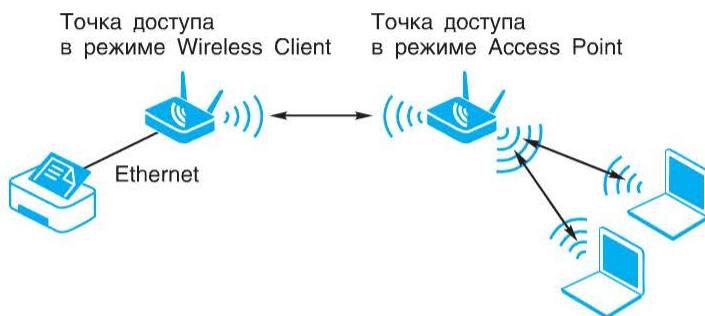


Рис. 8.25. Режим беспроводного клиента

Режим моста (Bridge) (рис. 8.26) позволяет подключить к беспроводной сети от одного до нескольких устройств, не имеющих беспроводных интерфейсов. Этот режим удобно использовать, например, при подключении таких устройств, как принтеры или игровые консоли, имеющие только порт Ethernet.

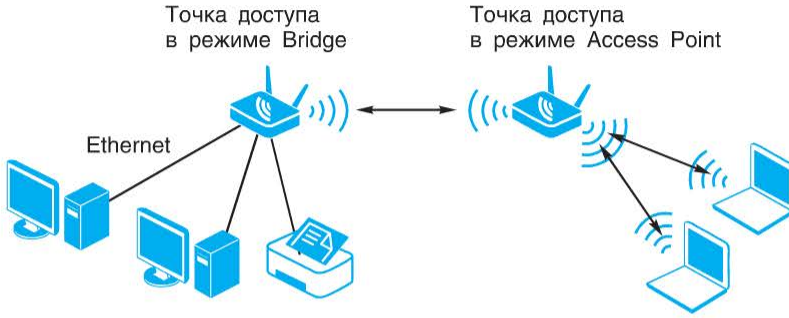


Рис. 8.26. Режим моста

Режимы WDS и WDS with AP были рассмотрены в 8.3. Отличием режимов WDS/WDS with AP и Bridge является то, что при работе в режиме Bridge точка доступа устанавливает соединение только с одной точкой доступа, работающей в режиме Access Point. Другими словами, режим Bridge служит для подключения устройств с интерфейсом Ethernet к беспроводной сети, а режимы WDS/WDS with AP служат для соединения точек доступа и построения распределенных сетей.

В домашних сетях или сетях небольших офисов в случае, когда зона покрытия точки доступа или беспроводного маршрутизатора ограничена какими-либо препятствиями, например стенами, для ее расширения и обеспечения доступности связи во всем помещении можно использовать точку доступа, настроенную на работу в режиме *повторителя* (*Repeater*) (рис. 8.27).

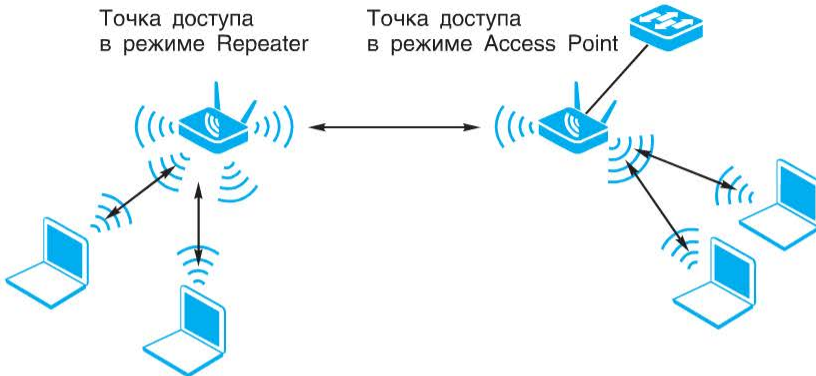


Рис. 8.27. Режим повторителя

Аналогично проводному повторителю беспроводной повторитель получает сигналы на свой беспроводной интерфейс в определенном радиочастотном канале, усиливает и ретранслирует их в том же самом канале, не изменяя кадр. Несмотря на расширение зоны покрытия, использование точки доступа в режиме повторителя приводит к уменьшению пропускной способности

беспроводной сети, поскольку повторитель должен принять и передать один и тот же кадр, что приводит к удвоению числа передаваемых в беспроводной сети кадров. В связи с этим рекомендуется использовать в сети не более трех повторителей. Существует еще одно ограничение при использовании режима повторителя: в сети должно использоваться однотипное оборудование (вплоть до версии прошивки) одного производителя.

8.6. Организация электропитания точек доступа

Одним из важных вопросов при развертывании беспроводной сети является организация электропитания точек доступа. Для достижения лучшего уровня беспроводного сигнала точки доступа могут устанавливаться на потолке, крыше или в других труднодоступных местах, где поблизости нет источника питания. Задача подачи питания на точку доступа в этом случае может быть решена с помощью технологии PoE (Power over Ethernet).*



Рис. 8.28. Подключение и организация питания точек доступа

При организации питания точек доступа с поддержкой PoE лучшим решением будет использование коммутатора с поддержкой PoE, поскольку при этом будет обеспечено одновременно и подключение, и питание точки доступа. Если точки доступа соединены коммутатором без поддержки PoE, для подачи питания к точке доступа с PoE можно использовать инжектор

*Подробное описание технологии PoE приведено в первой части курса «Основы сетевых технологий», доступного для изучения на портале дистанционного обучения и сертификации D-Link (<http://learn.dlink.ru>).

РoЕ. Однако это решение неудобно в том случае, если требуется организовать питание нескольких точек доступа, поскольку при этом возрастает количество используемого оборудования. При подключении к коммутатору с поддержкой РoЕ точки доступа без поддержки РoЕ проблему подачи питания можно решить с помощью РoЕ-сплиттера (рис. 8.28).

При выборе оборудования РoЕ, предназначенного для питания точек доступа, обращайте внимание на их потребляемую мощность. Точки доступа 802.11n и 802.11ac с поддержкой РoЕ, работающие одновременно в обоих частотных диапазонах 2,4 и 5 ГГц, требуют высокой входной мощности, поэтому для организации их питания необходимо использовать коммутаторы и инжекторы стандарта IEEE 802.3at.

8.7. Сегментация беспроводной сети

Сегментация беспроводной сети позволяет повысить ее производительность и защищенность, разграничить доступ к ресурсам. В архитектуре WLAN идентификатор SSID определяет группу взаимодействующих между собой точек доступа и клиентских устройств. Для того чтобы устройства могли взаимодействовать друг с другом, в их настройках должны быть указаны одинаковые параметры (SSID, настройки безопасности). В беспроводной сети можно определить несколько SSID, например, на двухдиапазонных точках можно задавать разные SSID для беспроводных интерфейсов 2,4 и 5 ГГц. Если точка доступа поддерживает функцию Multiple SSID (Multi-SSID), то на базе любого ее физического беспроводного интерфейса может быть создано несколько виртуальных интерфейсов, поддерживающих разные SSID (количество виртуальных интерфейсов зависит от модели точки доступа). Таким образом, различные типы клиентов беспроводной сети (например, гости, сотрудники) или трафик отдельных приложений (например, голос или видео) можно объединить в логические группы на основе разных SSID.

Внимание: все виртуальные интерфейсы Multi-SSID, созданные на базе любого беспроводного интерфейса 2,4 или 5 ГГц, работают на одном канале (на канале физического интерфейса).

Клиенты, подключенные к беспроводным интерфейсам с разными SSID, могут передавать друг другу данные в пределах одной точки доступа. Для того чтобы трафик разных групп клиентов был полностью изолирован друг от друга, SSID беспроводных интерфейсов (физических и/или виртуальных) требуется привязать к разным виртуальным локальным сетям (VLAN)*. Таким образом, пара SSID/VLAN позволит разбить беспроводную сеть на сегменты, для каждого из которых определить свои настройки безопасности, контроля широковещательных сообщений и качества обслуживания (QoS).

* Подробное описание технологии VLAN см. «Технологии коммутации и маршрутизации в локальных компьютерных сетях». М.: Издательство МГТУ им. Н.Э. Баумана, 2013, а также на портале дистанционного обучения и сертификации D-Link (<http://learn.dlink.ru>).

Для выполнения сегментации сети на основе VLAN точки доступа должны поддерживать стандарт IEEE 802.1Q. Виртуальные локальные сети, построенные на основе стандарта IEEE 802.1Q, используют дополнительные поля кадра для хранения информации о принадлежности к VLAN при его перемещении по сети.

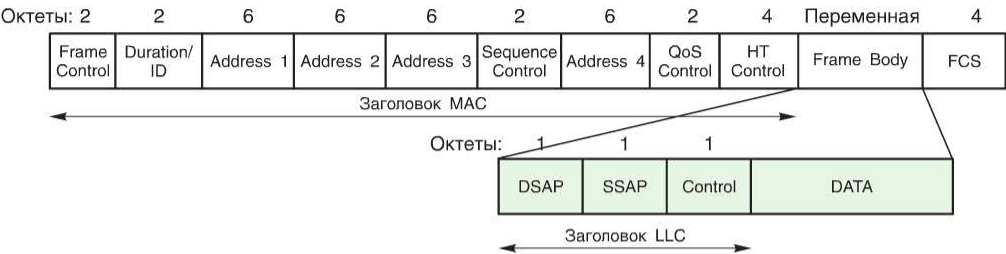
Напомним некоторые определения этого стандарта:

- *Tagging* (Маркировка кадра) — процесс добавления в заголовок кадра информации о принадлежности к 802.1Q VLAN.
- *Untagging* (Извлечение тега из кадра) — процесс извлечения (удаления) из заголовка кадра информации о принадлежности к 802.1Q VLAN.
- **VLAN ID (VID)** — идентификатор VLAN.
- **Port VLAN ID (PVID)** — идентификатор порта VLAN.

В Ethernet-кадрах тег 802.1Q добавляется в заголовок кадра MAC-подуровня и расширяет его на 4 байта. В кадре 802.11 тег добавляется после заголовка LLC-подуровня, следующего за заголовком MAC-подуровня (заголовок LLC в 802.11 обязателен в соответствии со спецификацией IEEE 802). Для того чтобы добавить в кадр информацию об идентификаторе VLAN, за трехоктетным заголовком LLC-подуровня должен следовать пятиоктетный заголовок SNAP, в поле «Type» которого установлено значение 0x8100. Это значение определяет, что кадр содержит тег протокола 802.1Q, который находится в двухоктетном поле, следующем за полем «Type» (рис. 8.29).

Точку доступа можно рассматривать как коммутатор, имеющий следующие порты: управление (Mgmt), локальная сеть (LAN), MSSID и WDS (ко-

Немаркированный кадр 802.11



Маркированный кадр 802.11

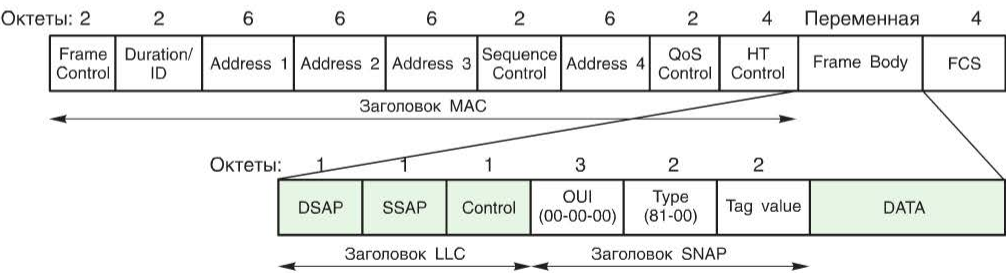


Рис. 8.29. Тег 802.1Q VLAN в кадре 802.11

личество портов MSSID и WDS зависит от модели точки доступа). Любой порт точки доступа может быть настроен как Tag (маркированный), Untag (немаркированный) или Not member. Функция Untag позволяет работать с сетевыми устройствами виртуальной сети, не понимающими тегов в заголовках кадров. Функция Tag позволяет настраивать VLAN между несколькими точками доступа или между точками доступа и коммутаторами, поддерживающими стандарт IEEE 802.1Q.

Функция Not member используется для указания портов, которые не включены в VLAN (рис. 8.30).

VLAN Settings

VLAN Status : ☒ Disable ☐ Enable

VLAN Mode : Static

VLAN List | Port List | **Add/Edit VLAN** | PVID Setting

VLAN ID (VID)	VLAN Name
Port	Select All Mgmt LAN
Untag	All <input type="radio"/> <input type="radio"/> <input type="radio"/>
Tag	All <input type="radio"/> <input type="radio"/> <input type="radio"/>
Not Member	All <input type="radio"/> <input type="radio"/> <input type="radio"/>
MSSID Port	Select All Primary S-1 S-2 S-3 S-4 S-5 S-6 S-7
Untag	All <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>
Tag	All <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>
Not Member	All <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>
WDS Port	Select All W-1 W-2 W-3 W-4 W-5 W-6 W-7 W-8
Untag	All <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>
Tag	All <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>
Not Member	All <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>

Рис. 8.30. Настройка VLAN на точке доступа D-Link DAP-2310

Каждый порт точки доступа имеет *идентификатор порта VLAN* (PVID). Этот параметр используется для того, чтобы определить, в какую VLAN точка доступа направит входящий немаркированный кадр из подключенного к порту сетевого сегмента, если кадр необходимо передать на другой порт. На точке доступа в заголовки всех немаркированных кадров беспроводных клиентов добавляется идентификатор VID, равный PVID порта MSSID, на который они были приняты (рис. 8.31). Этот механизм позволяет одновременно сосуществовать в одной сети устройствам с поддержкой и без поддержки стандарта IEEE 802.1Q.

Точки доступа, поддерживающие стандарт IEEE 802.1Q, хранят таблицу, связывающую идентификаторы портов PVID с идентификаторами VID сети. При этом каждый порт точки доступа может иметь только один PVID и столько идентификаторов VID, сколько поддерживает данная модель устройства.

Если на точке доступа не настроены VLAN, то все порты по умолчанию входят в одну VLAN с PVID=1 (рис. 8.32).

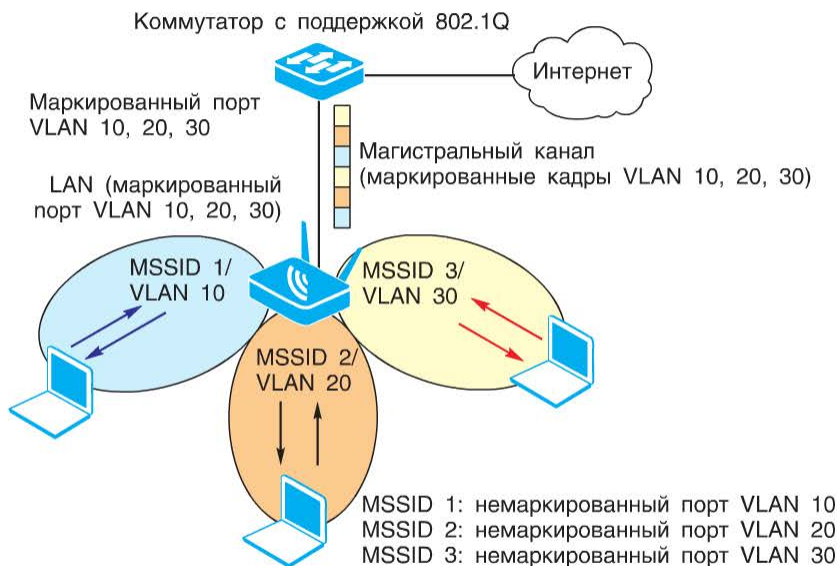


Рис. 8.31. Маркированные и немаркированные порты VLAN

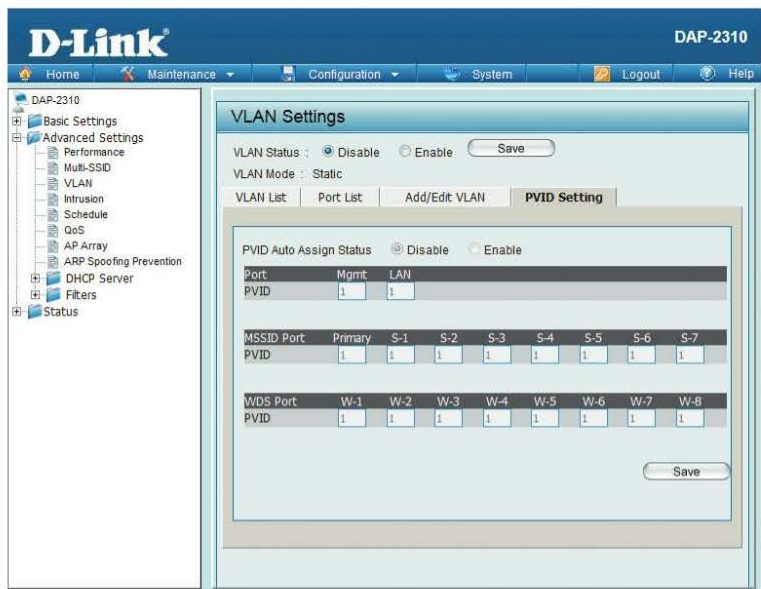


Рис. 8.32. Настройки PVID на точке доступа D-Link DAP-2310

Классификация кадра по принадлежности VLAN осуществляется следующим образом:

- а) если кадр не содержит информацию о VLAN (немаркированный кадр), то в его заголовок точка доступа добавляет тег с идентификатором VID, равным идентификатору PVID порта, через который этот кадр был принят;

б) если кадр содержит информацию о VLAN (маркированный кадр), то его принадлежность к конкретной VLAN определяется по идентификатору VID в заголовке кадра. Значение тега в нем не изменяется.

Если входящий кадр маркированный, точка доступа определяет, является ли входной порт членом той же VLAN путем сравнения идентификатора VID в заголовке кадра и набора идентификаторов VID, ассоциированных с портом, включая его PVID. Если нет, то кадр отбрасывается. Этот процесс называется *ingress filtering* (*входной фильтрацией*) и используется для поддержания пропускной способности на точке доступа путем отбрасывания кадров, не принадлежащих той же VLAN, что и входной порт, на стадии их приема. Если кадр немаркированный, входная фильтрация не выполняется.

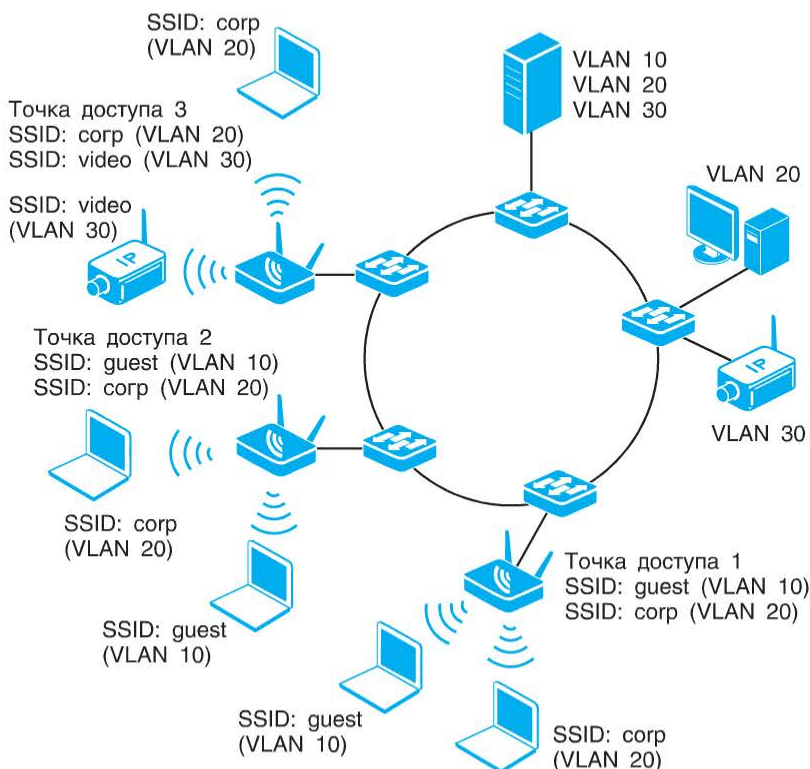


Рис. 8.33. Сеть с VLAN, включающими проводных и беспроводных клиентов

Далее определяется, является ли порт назначения членом той же VLAN. Если нет, то кадр отбрасывается. Если же выходной порт входит в данную VLAN, то точка доступа передает кадр в подключенный к нему сегмент сети.

Если выходной порт является немаркированным (Untag), то он будет извлекать (удалять) тег 802.1Q из заголовков всех выходящих через него маркированных кадров. Если выходной порт настроен как маркированный

(Tag), он будет сохранять тег 802.1Q в заголовках всех выходящих через него маркированных кадров.

В сетях масштаба предприятия обычно применяются как проводные, так и беспроводные сегменты сети. В этом случае клиенты беспроводной сети могут быть выделены в отдельную VLAN или стать членами соответствующих VLAN проводной части сети (рис. 8.33).

Рассмотрим примеры настройки сегментации беспроводной сети с использованием VLAN.

Пример 1: офисная беспроводная сеть построена на основе двухдиапазонной точки доступа D-Link DAP-2660. Сеть необходимо разбить на два сегмента: для гостей (guest) и сотрудников (sales). Сегмент с SSID sales привязан к VLAN 10 (VID 10), сегмент с SSID guest привязан к VLAN 20 (VID 20). Клиентское оборудование сотрудников включает как однодиапазонные, так и двухдиапазонные устройства.

Для повышения производительности сети двухдиапазонное оборудование сотрудников желательно подключать к точке доступа в диапазоне 5 ГГц. Оборудование гостей всегда должно подключаться в диапазоне 2,4 ГГц (рис. 8.34).



Рис. 8.34. Схема сети для примера 1

Для того чтобы двухдиапазонное клиентское оборудование сотрудников подключалось к точке доступа в диапазоне 5 ГГц, требуется настроить на точке доступа функцию *band steering* (ее описание приведено в 8.9 «Функции оптимизации производительности»).

Настройка точки доступа осуществляется следующим образом.

Шаг 1. Создание сегмента беспроводной сети с SSID sales в диапазонах частот 2,4 и 5 ГГц:

1) зайти во вкладку *Wireless Settings*;

2) выполнить следующие настройки сначала для диапазона 2,4 ГГц (рис. 8.35), затем для диапазона 5 ГГц (рис. 8.36): в поле *SSID* ввести *sales*, в выпадающем меню *Authentication* выбрать *WPA-Personal*, в поле *PassPhrase* ввести пароль *PasswordDlink* и повторить его в поле *Confirm PassPhrase*, нажать кнопку *Save*.



Рис. 8.35. Создание сегмента с SSID sales в диапазоне 2,4 ГГц

Шаг 2. Настройка функции *band steering*. Зайти во вкладку *Advanced Settings* → *Wireless Resource*. В выпадающем меню *Wireless band* выбрать 5GHz, в *Band Steering* — *Enable* и нажать кнопку *Save*.

Шаг 3. Создание сегмента беспроводной сети с SSID guest в диапазоне частот 2,4 ГГц (рис. 8.37, 8.38):

- 1) зайти во вкладку *Advanced Settings* → *Multi-SSID*;
- 2) активизировать функцию *Multi-SSID*, поставив галочку в *Enable Multi-SSID*;
- 3) в выпадающем списке *Index* выбрать *SSID1*;
- 4) в поле *SSID* ввести *guest*;
- 5) в выпадающем меню *Security* выбрать *WPA-Personal*;
- 6) в поле *PassPhrase* ввести пароль *PasswordGuest* и повторить его в поле *Confirm PassPhrase*;
- 7) нажать кнопку *Add*.

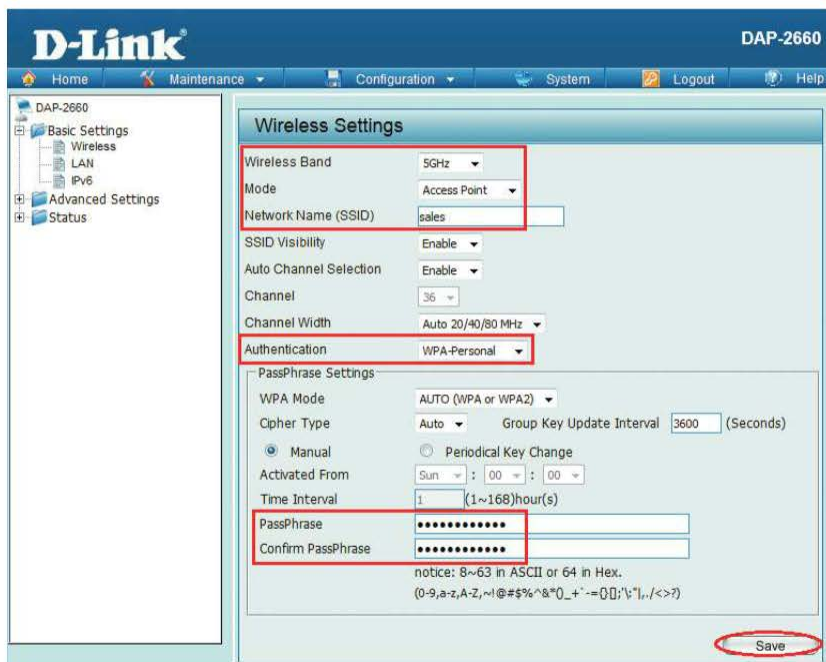


Рис. 8.36. Создание сегмента с SSID sales в диапазоне 5 ГГц

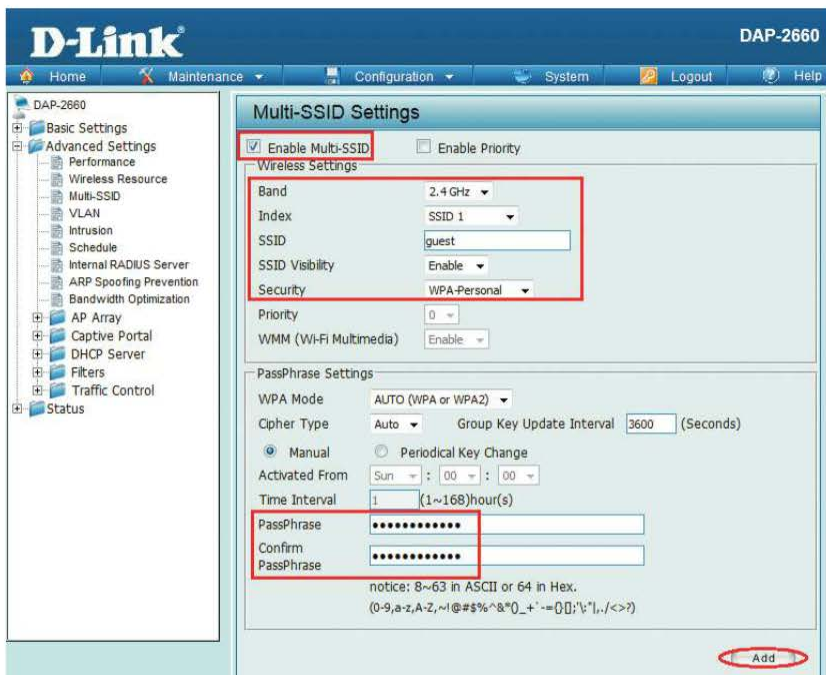


Рис. 8.37. Создание сегмента с SSID guest в диапазоне 2,4 ГГц


Index	SSID	Band	Encryption	Delete
Primary SSID	sales	2.4 GHz	WPA2-Auto-Personal	
Multi-SSID1(Edit)	guest	2.4 GHz	WPA2-Auto-Personal	

Рис. 8.38. Созданные сегменты с SSID guest и SSID sales

Шаг 4. Настройка привязки SSID и VLAN. Трафик с *SSID guest* должен направляться в *VLAN 20* (VID 20), а с *SSID sales* — в *VLAN 10* (VID 10). MSSID-порты Primary 2,4 ГГц и Primary 5 ГГц являются немаркированными портами VLAN sales. Порт MSSID 1 (S-1) является немаркированным портом VLAN guest:

- 1) зайти во вкладку *Advanced Settings* → *VLAN* и включить поддержку VLAN, выбрав *Enable* в поле *VLAN Status*. Нажать кнопку *Save*;
- 2) удалить порты из VLAN по умолчанию (default). Во вкладке *VLAN List* нажать *Edit*;
- 3) в открывшемся окне установить галочки *Not Member* для MSSID-портов *Primary* и *S-1* в диапазоне 2,4 ГГц и для *Primary* в диапазоне 5 ГГц. Нажать кнопку *Save* (рис. 8.39);

Внимание: заводские установки по умолчанию назначают все порты точки доступа в default VLAN с VID = 1. Перед созданием новой VLAN необходимо удалить из default VLAN все порты, которые требуется сделать немаркированными членами новой VLAN. Немаркированные порты не могут одновременно быть членами нескольких VLAN.

- 4) выбрать вкладку *Add/Edit VLAN*:
 - в поле *VLAN ID (VID)* ввести 10, в поле *VLAN Name* — 10. MSSID-порты *Primary* 2,4 ГГц и *Primary* 5 ГГц включить в VLAN 10 как немаркированные и нажать кнопку *Save* (рис. 8.40);
 - в поле *VLAN ID (VID)* ввести 20, в поле *VLAN Name* — 20. Порт MSSID 1 (S-1) в диапазоне 2,4 ГГц включить в VLAN 20 как немаркированный и нажать кнопку *Save* (рис. 8.41).

Шаг 5. Проверка созданных VLAN. Зайти во вкладку *Advanced Settings* → *VLAN* → *VLAN List* (рис. 8.42).

Шаг 6. Назначение PVID немаркированным MSSID-портам *Primary* и *S-1* в диапазоне 2,4 ГГц, *Primary* в диапазоне 5 ГГц. Выбрать вкладку *PVID Setting*. В полях *Primary* 2,4 ГГц и *Primary* 5 ГГц ввести 10, в поле *S-1* диапазона 2,4 ГГц — 20. Нажать кнопку *Save* (рис. 8.43).

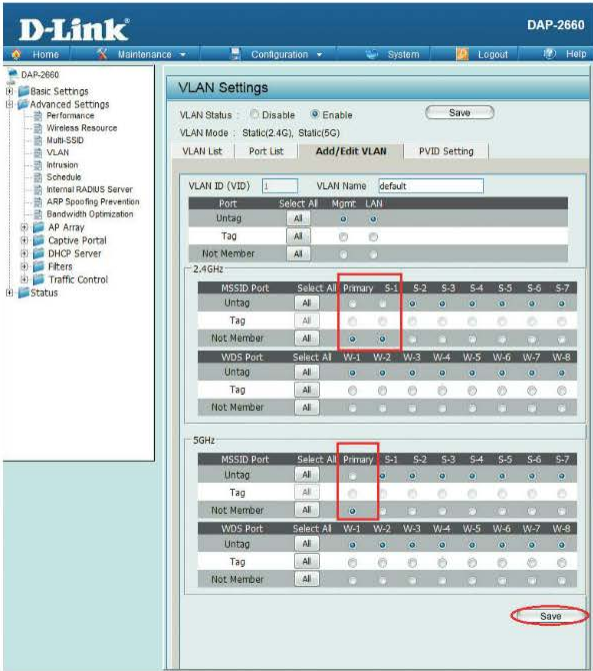


Рис. 8.39. Удаление портов из VLAN по умолчанию

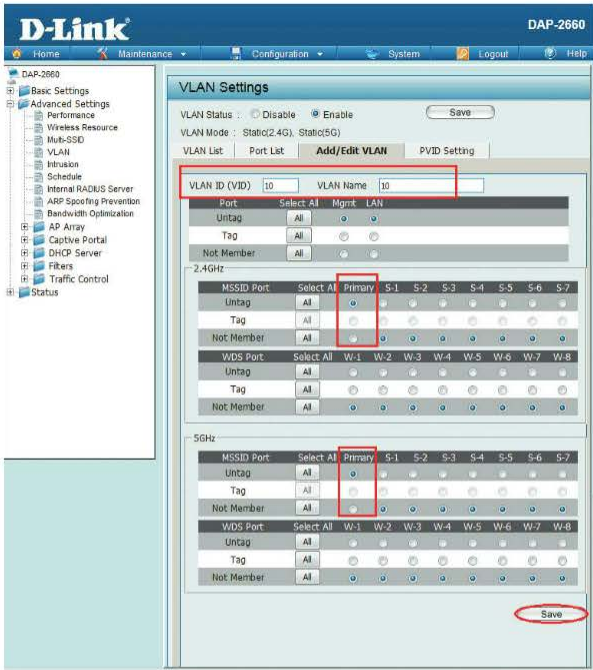


Рис. 8.40. Создание VLAN 10

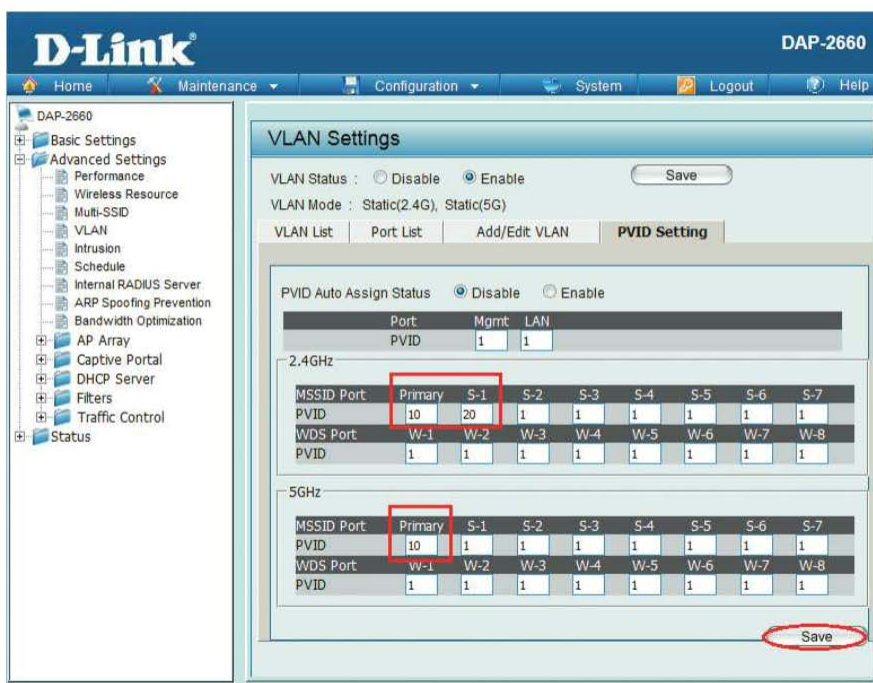


Рис. 8.43. Настройка PVID

Пример 2: офисная беспроводная сеть построена на основе двух однодиапазонных точек доступа D-Link DAP-2310, соединенных между собой с помощью беспроводной распределительной системы (WDS). Точки доступа работают в режиме WDS with AP, чтобы иметь возможность подключать беспроводных клиентов. Сеть необходимо разбить на два сегмента: для гостей (guest) и сотрудников (sales). Сегмент с SSID guest привязан к VLAN guest (VID 10), сегмент с SSID sales привязан к VLAN sales (VID 20) (рис. 8.44). Настройка точек доступа для работы в режиме WDS приводиться не будет, так как предполагается, что эти настройки уже сделаны ранее.

Настройка точек доступа AP1 и AP2 осуществляется следующим образом.

Шаг 1. Включение поддержки функции Multi-SSID и создание двух сегментов беспроводной сети с SSID *guest* и *sales*:

- 1) зайти во вкладку *Advanced Settings* → *Multi-SSID*;
- 2) активизировать функцию *Multi-SSID*, поставив галочку в *Enable Multi-SSID*;
- 3) в выпадающем списке *Index* выбрать *SSID1*;
- 4) в поле *SSID* ввести *guest*;
- 5) в выпадающем меню *Security* выбрать *WPA-Personal*;
- 6) в поле *PassPhrase* ввести пароль *PasswordDlink* и повторить его в поле *Confirm PassPhrase*;
- 7) нажать кнопку *Add* (рис. 8.45).



Рис. 8.44. Схема сети для примера 2

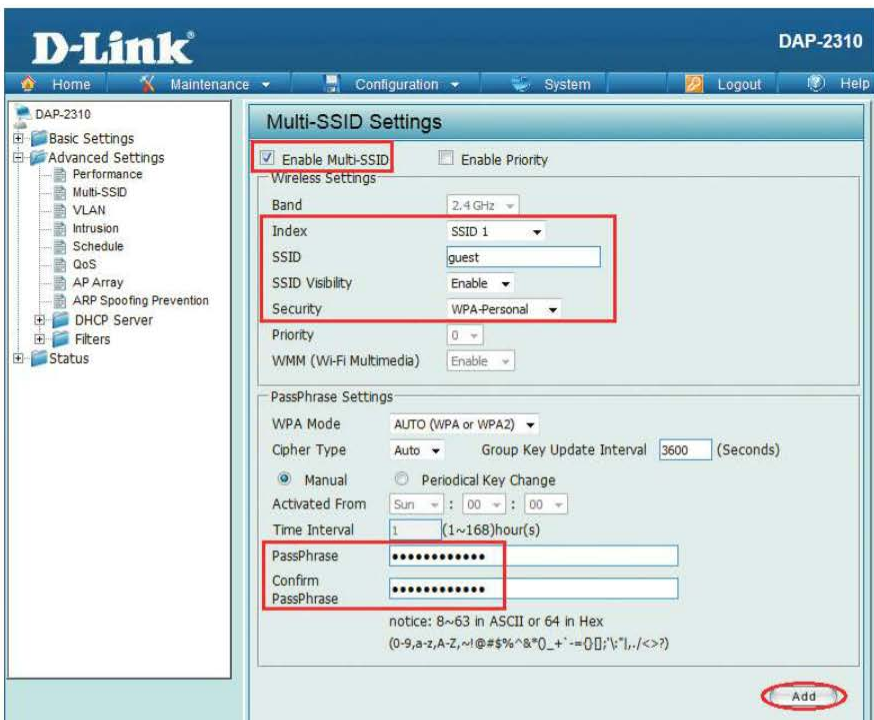


Рис. 8.45. Создание сегмента сети с SSID guest

- Аналогичным образом создать *SSID2 sales*:
- 1) в выпадающем списке *Index* ввести *SSID2*;
 - 2) в поле *SSID* ввести *sales*;
 - 3) в выпадающем меню *Security* выбрать *WPA-Personal*;
 - 4) в поле *PassPhrase* ввести пароль *DlinkQwerty* и повторить его в поле *Confirm PassPhrase*;
 - 5) нажать кнопку *Add*;
 - 6) сохранить созданные SSID, нажав кнопку *Save* (рис. 8.46).

Index	SSID	Band	Encryption	Delete
Primary SSID	Dlink_WDS	2.4 GHz	WPA2-Auto-Personal	
Multi-SSID1	guest	2.4 GHz	WPA2-Auto-Personal	
Multi-SSID2	sales	2.4 GHz	WPA2-Auto-Personal	

Save

Рис. 8.46. Созданные сегменты с SSID guest и SSID sales

Шаг 2. Настройка привязки SSID и VLAN. Трафик с *SSID guest* должен направляться в *VLAN guest* (VID 10), а с *SSID sales* — в *VLAN sales* (VID 20).

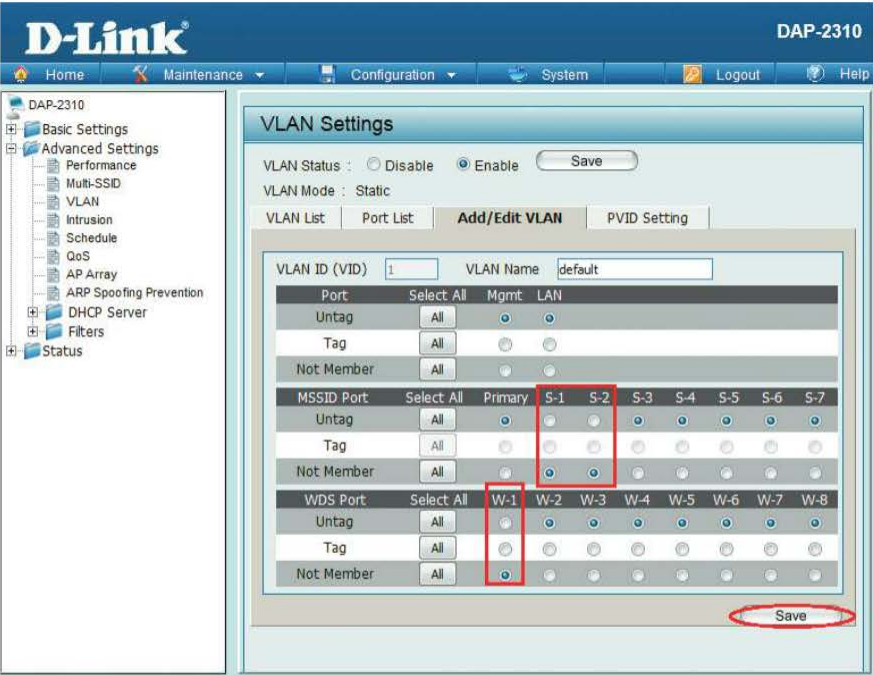


Рис. 8.47. Удаление портов из VLAN по умолчанию

Порты MSSID 1 (S-1) и MSSID 2 (S-2) обеих точек доступа являются немаркированными портами VLAN guest и VLAN sales соответственно. Порт WDS (W-1) обеих точек доступа является маркированным портом VLAN guest и VLAN sales:

1) зайти во вкладку *Advanced Settings* → *VLAN* и включить поддержку VLAN, выбрав *Enable* в поле *VLAN Status*. Нажать кнопку *Save*;

2) удалить порты из VLAN по умолчанию (default). Во вкладке *VLAN List* нажать *Edit*;

3) в открывшемся окне установить галочки *Not Member* для портов *S-1*, *S-2* и *W-1*, нажать кнопку *Save* (рис. 8.47);

4) выбрать вкладку *Add/Edit VLAN*:

- в поле *VLAN ID (VID)* ввести 10, в поле *VLAN Name* — *guest*. WDS-порт *W-1* включить в VLAN как маркированный, MSSID-порт *S-1* — как немаркированный. Нажать кнопку *Save* (рис. 8.48);

- аналогично в поле *VLAN ID (VID)* ввести 20, в поле *VLAN Name* — *sales*. Настроить WDS-порт *W-1* как маркированный, MSSID-порт *S-2* как немаркированный. Нажать кнопку *Save*.

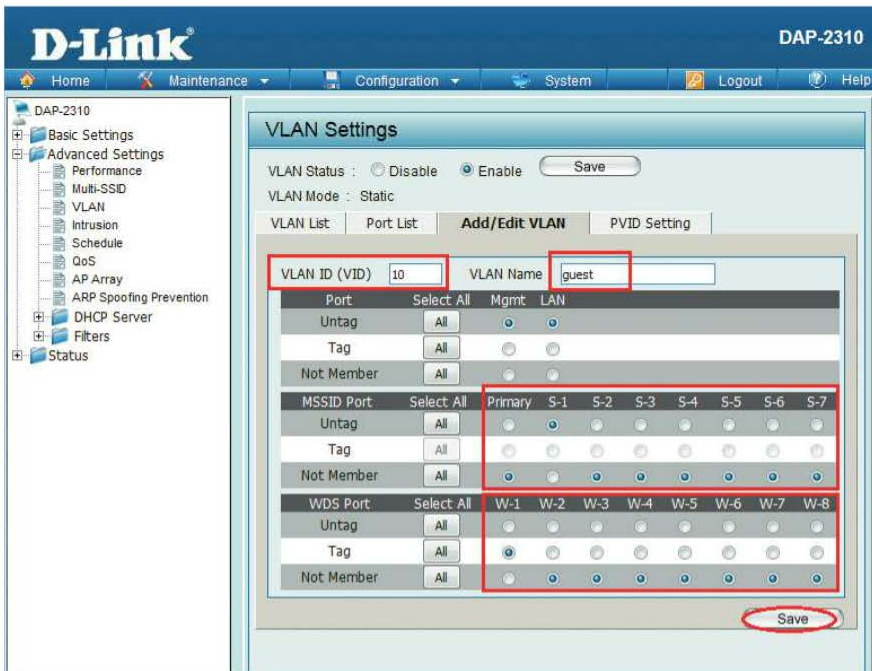


Рис. 8.48. Создание VLAN guest

Шаг 3. Проверка созданных VLAN. Зайти во вкладку *Advanced Settings* → *VLAN* → *VLAN List* (рис. 8.49).

CW_{min} и CW_{max}) к каналу связи различаются для каждой очереди (табл. 8.2). Кадры из высокоприоритетной очереди имеют бóльшую вероятность получить возможность передачи (TXOP) в процессе состязания за беспроводную среду, так как имеют наименьшие значения арбитражного межкадрового интервала (AIFS), CW_{min} и CW_{max} . Если кадры из разных очередей создают внутреннюю коллизию, то первым будет передан кадр с наивысшим приоритетом, а кадр с меньшим приоритетом изменит значение таймера обратного отсчета так же, как это делается при возникновении внешней коллизии.

Таблица 8.2. Категории доступа WMM

Категории доступа	Описание	Приоритет 802.1D	AIFS	CW_{min}	CW_{max}
WMM Voice Priority	Наивысший приоритет. Трафик VoIP и другой трафик, требующий минимальных задержек передачи	7, 6	2	$(aCW_{min}+1)/4-1$	$(aCW_{min}+1)/2-1$
WMM Video Priority	Приоритетная передача видеотрафика по сравнению с трафиком данных	5, 4	2	$(aCW_{min}+1)/2-1$	aCW_{min}
WMM Best Effort Priority	Трафик устаревших устройств или устройств без поддержки QoS. Трафик, не чувствительный к задержкам, такой как просмотр Web-страниц	0, 3	3	aCW_{min}	aCW_{max}
WMM Background Priority	Низкоприоритетный трафик, не имеющий жестких требований к задержкам и полосе пропускания, такой как загрузка файлов, сетевая печать	2, 1	7	aCW_{min}	aCW_{max}

Кадры данных, в которых отсутствует информация о приоритете, привязываются к категории AC_BE. Кадры управления, в которых отсутствует поле QoS Control, привязываются к категории AC_VO.

QoS в беспроводной сети можно применять как к нисходящему потоку данных, так и к восходящему. Любой беспроводной клиент, сертифицированный на соответствие WMM, может реализовывать QoS в восходящем направлении, т. е. к точке доступа. При этом клиент в зависимости от его реализации самостоятельно определяет механизм приоритизации пакетов. Точки доступа D-Link можно настроить для обеспечения QoS во всех направлениях: от клиента и к клиенту (рис. 8.52).

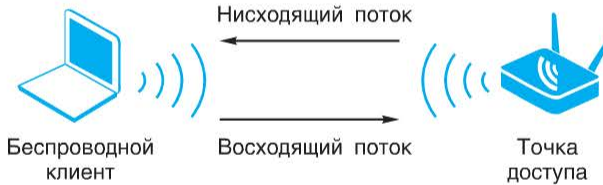


Рис. 8.52. Направления трафика

В зависимости от модели точки доступа могут выполнять приоритизацию входящего трафика, распределять исходящий трафик по очередям приоритетов, управлять полосой пропускания для входящих и исходящих потоков данных на беспроводных интерфейсах. На проводном интерфейсе Ethernet все исходящие кадры помещаются в одну общую очередь типа FIFO (First Input, First Output, первым пришел — первым ушел).

Поскольку не все клиенты поддерживают функционал QoS или если у администратора сети нет уверенности в том, что механизм QoS клиента

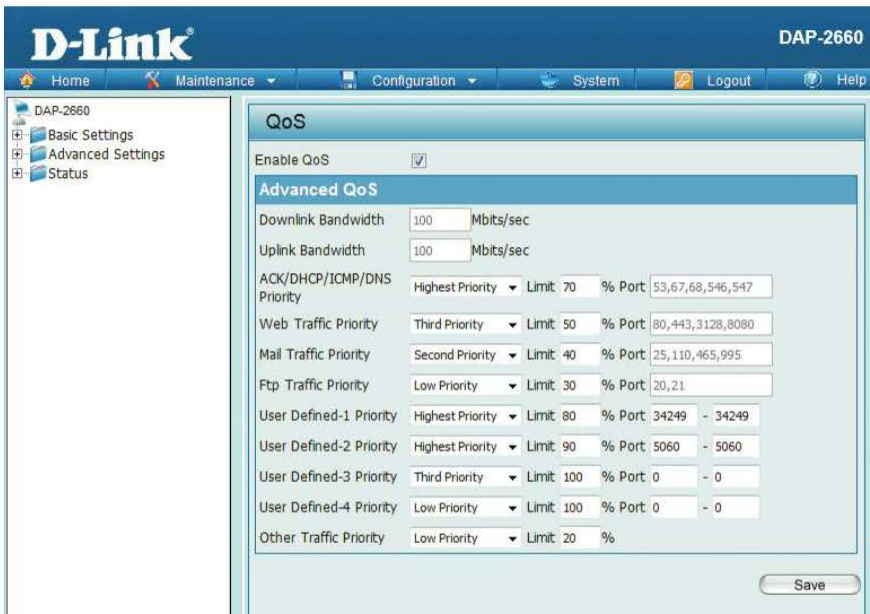


Рис. 8.53. Настройка правил QoS на точке доступа D-Link DAP-2660

правильно приоритизирует кадры, на точках доступа можно настраивать правила, позволяющие помещать трафик соответствующих приложений или клиентов в нужные очереди приоритетов (рис. 8.53). Некоторые модели точек доступа также предоставляют возможность регулировать интенсивность входящего и исходящего трафика на своих беспроводных интерфейсах. Ограничить скорость соединения можно для всего трафика, входящего на беспроводной порт и исходящего через него, для трафика конкретных приложений, определенных администратором сети, и для трафика соответствующих клиентов.

Для обеспечения требуемого качества обслуживания в беспроводной сети, состоящей из нескольких точек доступа, одинаковые настройки функций QoS необходимо установить на всех точках доступа.

8.9. Функции оптимизации производительности

Одной из функций, позволяющих повысить производительность беспроводной сети, является функция *band steering*, поддерживаемая только двухдиапазонными точками доступа. Она определяет среди ассоциирующихся с точкой доступа устройств двухдиапазонных клиентов и подключает их в диапазоне 5 ГГц. Существует три режима работы этой функции. На точках доступа D-Link функция *band steering* работает в режиме 5G Preferred. Напомним, что в обычном режиме работы перед подключением к точке доступа беспроводные клиенты проводят активное или пассивное сканирование каждого канала с целью определения доступных точек доступа. В ходе пассивного сканирования клиент прослушивает каждый канал в течение определенного периода времени на предмет обнаружения передаваемых точками доступа сигнальных кадров (Beacon). При активном сканировании клиент последовательно отправляет широкополосные кадры пробного запроса (*Probe request*) в каждый из проверяемых каналов и ждет ответ на пробный запрос (*Probe response*) от точки доступа.

При включении функции *band steering* точка доступа скрывает SSID в рассылаемых сигнальных кадрах (Beacon), что вынуждает беспроводных клиентов выполнять активное сканирование. Если за короткий период времени точка доступа получает пробный запрос от одного и того же клиента в обоих частотных диапазонах 2,4 и 5 ГГц, то прежде чем подключить клиента в диапазоне 5 ГГц, функция *band steering* рассматривает несколько параметров: клиент будет подключен в диапазоне 5 ГГц, если значение уровня его сигнала (RSSI) больше порогового значения, установленного администратором сети, и/или скорость передачи клиента больше установленной пороговой скорости. Также принимается во внимание текущая загрузка каждого диапазона точки доступа. Функция *band steering* будет подключать клиентов в диапазоне 5 ГГц, если на данной точке доступа разница между количеством клиентов, подключенных в диапазоне 5 ГГц и в диапазоне 2,4 ГГц, больше некоторого заранее определенного значения или в диапазоне 5 ГГц не превышен лимит подключаемых клиентов. Если функция *band steering* принимает

решение о подключении клиента в диапазоне 5 ГГц, точка доступа отправляет клиенту ответ на пробный запрос в диапазоне 5 ГГц, а в диапазоне 2,4 ГГц ответ на пробный запрос не отправляется.

Если точка доступа получает от клиента пробный запрос только в диапазоне 2,4 ГГц, то она отправляет ему ответ на пробный запрос только в этом диапазоне (рис. 8.54, 8.55).

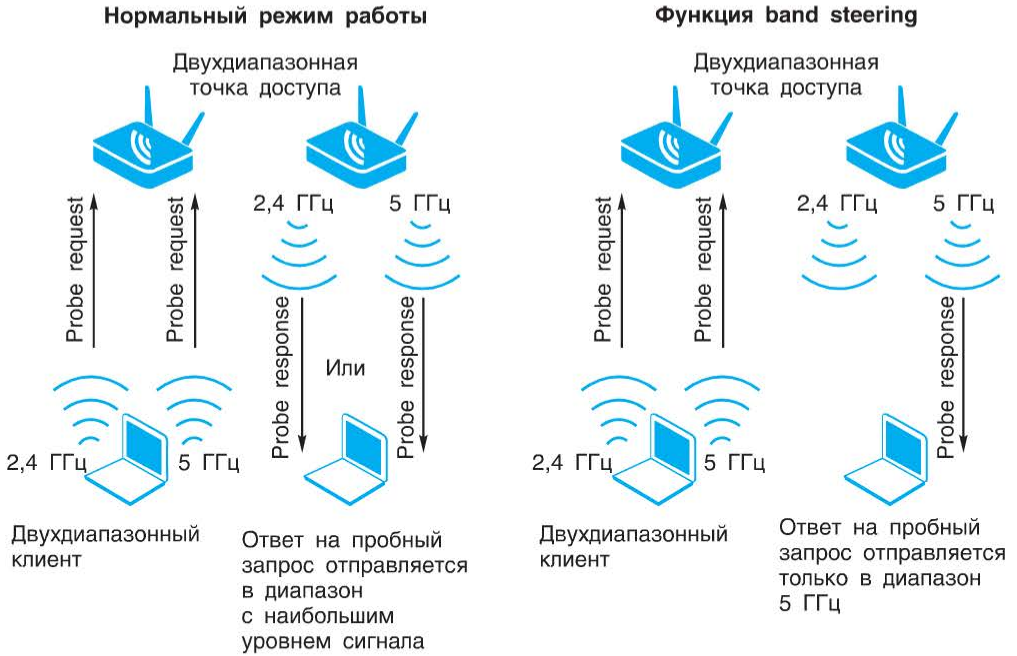


Рис. 8.54. Функция *band steering*

Таким образом, функция *band steering* повышает производительность сети за счет снижения межканальной интерференции, увеличения полосы пропускания в диапазоне 2,4 ГГц для однодиапазонных клиентов (вследствие сокращения общего количества клиентов) и в диапазоне 5 ГГц для двухдиапазонных клиентов (поскольку спектр диапазона 5 ГГц шире по сравнению с 2,4 ГГц).

Для оптимизации процесса ассоциации клиентов между членами группы точек доступа может использоваться функция *балансировки нагрузки* (*load balancing*). Она полезна в том случае, если точки доступа испытывают перегрузку вследствие переполнения приемных буферов устройств в любом из поддерживаемых частотных диапазонов. Балансировка нагрузки может выполняться как с помощью ограничения количества клиентов, подключаемых к точке доступа, так и на основе данных об использовании полосы пропускания канала.

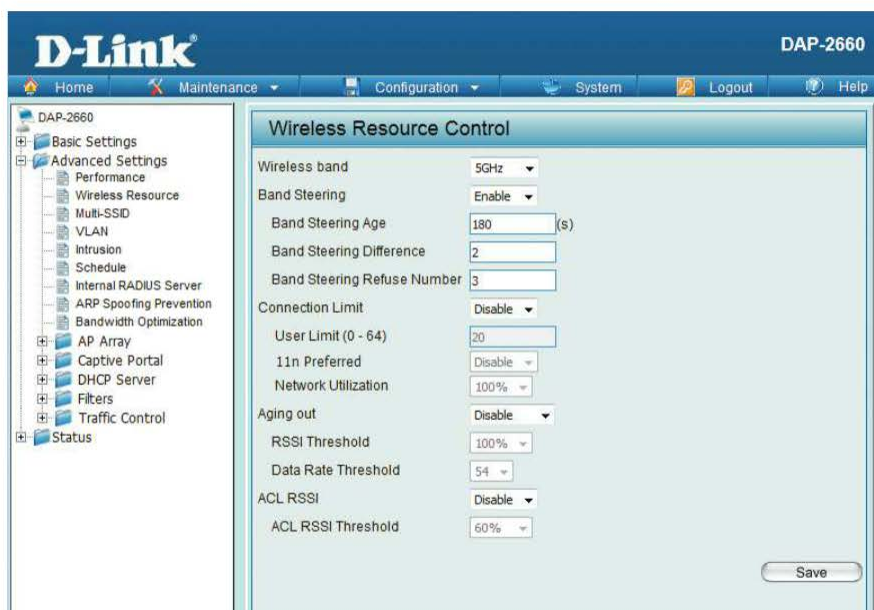


Рис. 8.55. Настройка функции *band steering* на точке доступа D-Link DAP-2660



Рис. 8.56. Балансировка нагрузки на основе использования полосы пропускания

Второй способ является более эффективным, так как отражает текущую доступную полосу пропускания (рис. 8.56). Выполнять балансировку нагрузки на основе количества клиентов не рекомендуется, так как не все ассоциированные с точкой доступа клиенты могут активно работать в сети. Помимо этого в данном методе не учитывается интерференция, присутствующая в канале.

8.10. Функции безопасности

В беспроводной сети любая станция, находящаяся в пределах радиосвязи с другими устройствами, может передавать и получать данные. Для обеспечения контроля над подключениями и предотвращения доступа к информации неавторизованных пользователей в беспроводной сети требуется настройка различных протоколов и технологий обеспечения безопасности.

8.10.1. Аутентификация и конфиденциальность данных

Настройки аутентификации и конфиденциальности данных по умолчанию во всех беспроводных устройствах отсутствуют, т. е. по умолчанию проверка подлинности пользователя и шифрование данных не выполняются. Для того чтобы обеспечить аутентификацию и конфиденциальность данных в беспроводной сети, на всех ее устройствах необходимо выполнить настройку параметров соответствующих протоколов безопасности.

Беспроводные устройства D-Link сертифицированы на соответствие требованиям программ сертификации WPA/WPA2. Напомним, что программы сертификации WPA/WPA2 представляют собой набор функций безопасности, которые позволяют решить большинство задач обеспечения защиты сетей 802.11. Начиная с 2006 года соответствие требованиям WPA2 является обязательным для всех устройств Wi-Fi CERTIFIED. Для обеспечения конфиденциальности данных в WPA используется протокол шифрования TKIP, в WPA2 — более криптоустойчивый протокол шифрования CCMP, основанный на алгоритме шифрования AES. Аутентификация в WPA/WPA2 выполняется на основе протоколов IEEE 802.1X с EAP для корпоративных пользователей (режим Enterprise) и PSK для домашних пользователей или пользователей небольших офисов (режим Personal).



Рис. 8.57. Режим WPA/WPA2-Personal

Для использования режима WPA/WPA2-Personal не требуется никакого дополнительного оборудования кроме точки доступа и клиентского устройства (рис. 8.57). Ключ шифрования в этом режиме получают из SSID и парольной фразы, введенной в настройках устройств. Для повышения безопасности сети рекомендуется использовать сложную парольную фразу и как можно чаще обновлять ее.

Режим WPA/WPA2-Enterprise предназначен для корпоративных сетей, в которых функционируют выделенные серверы аутентификации. Этот режим

основан на использовании протокола IEEE 802.1X с EAP и включает возможности мониторинга и управления трафиком, определения прав доступа пользователей, включая предоставление гостевого доступа (рис. 8.58).

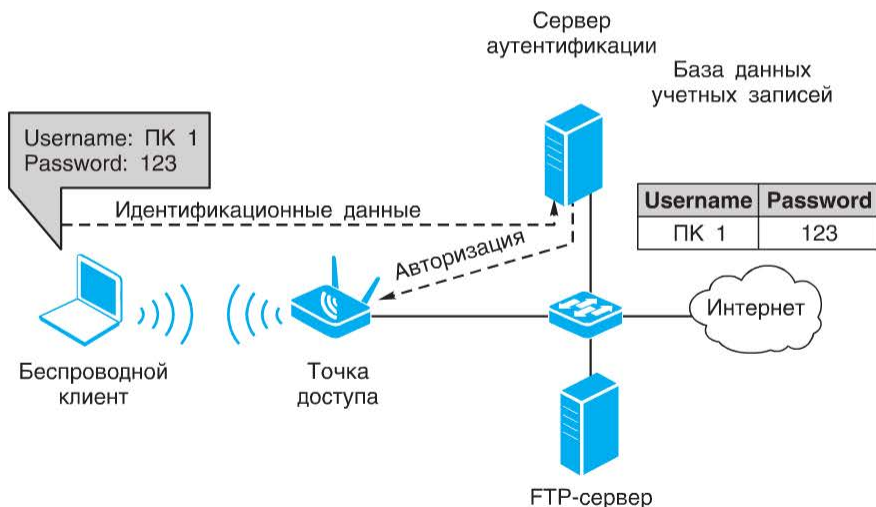


Рис. 8.58. Аутентификация в режиме WPA/WPA2-Enterprise с помощью сервера аутентификации

Беспроводные сети зачастую используются для предоставления гостевого доступа к общедоступным ресурсам, например Интернету. Гостевой трафик должен быть изолирован от трафика сотрудников компании в случае предоставления гостевого доступа в офисной или корпоративной сети или от трафика домашних пользователей, если доступ в Интернет надо предоставить друзьям, пришедшим в гости. В любом случае для гостевой беспроводной сети надо назначить собственный идентификатор SSID и для изоляции трафика привязать его к отдельной VLAN. С помощью списков контроля доступа (ACL), настраиваемых на маршрутизаторах, коммутаторах или контроллерах, используемых в сети, можно управлять потоком данных гостевого трафика и ограничивать доступ гостей к ресурсам сети. Посетители должны использовать идентификационную информацию (логин и пароль), которая позволит им авторизоваться только в гостевой сети.

Некоторые модели точек доступа и беспроводные контроллеры D-Link позволяют организовать гостевой доступ с помощью функции *Captive portal*. Эта функция чаще всего используется при организации доступа в Интернет через сети Wi-Fi в гостиницах, бизнес-центрах, ресторанах и т. п. *Captive portal* представляет собой Web-сервис, предназначенный для аутентификации пользователей при их попытке подключиться к Интернет: как только пользователь открывает Web-браузер и вводит в адресной строке адрес какого-либо сайта, его запрос автоматически перенаправляется на стартовую страницу портала,

находящуюся на точке доступа или беспроводном контроллере. На этой странице пользователь должен ввести свою идентификационную информацию (рис. 8.59).

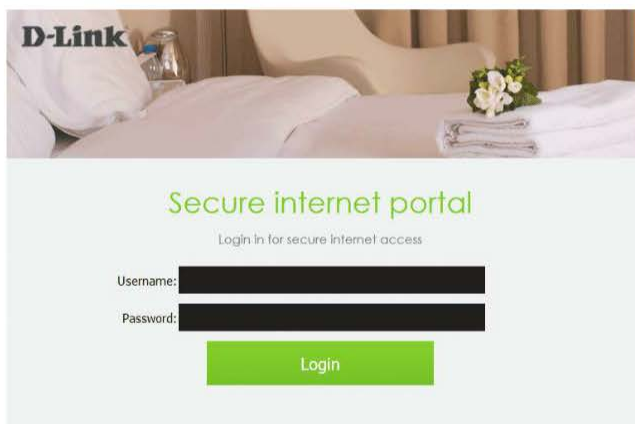


Рис. 8.59. Интерфейс аутентификации *Captive portal* на устройстве D-Link

После успешной авторизации, которая может выполняться как с использованием локальной базы данных, так и с использованием сервера аутентификации, клиенту разрешается доступ в Интернет.

При использовании *Captive portal* дополнительно можно настроить время пребывания пользователя в сети и ограничивать скорость его подключения (рис. 8.60, 8.61).

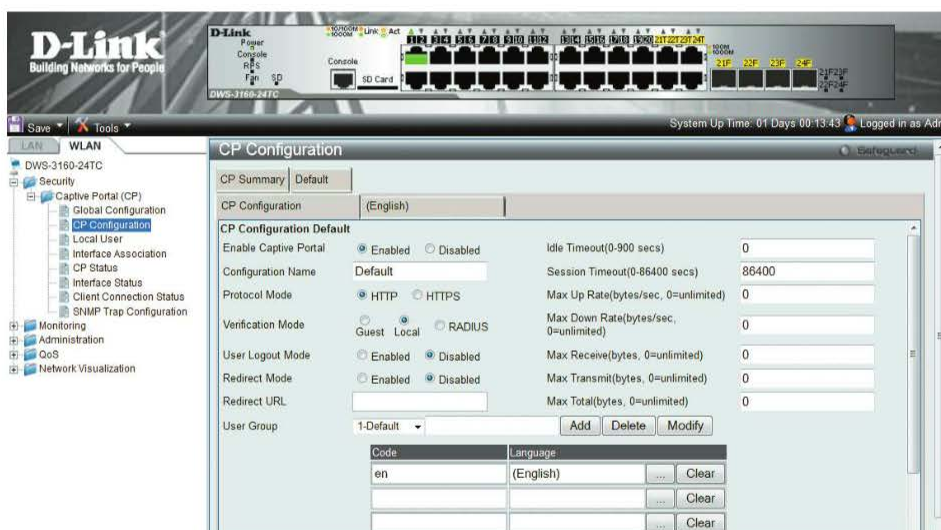


Рис. 8.60. Настройка *Captive portal* на беспроводном коммутаторе D-Link DWS-3160-24TC

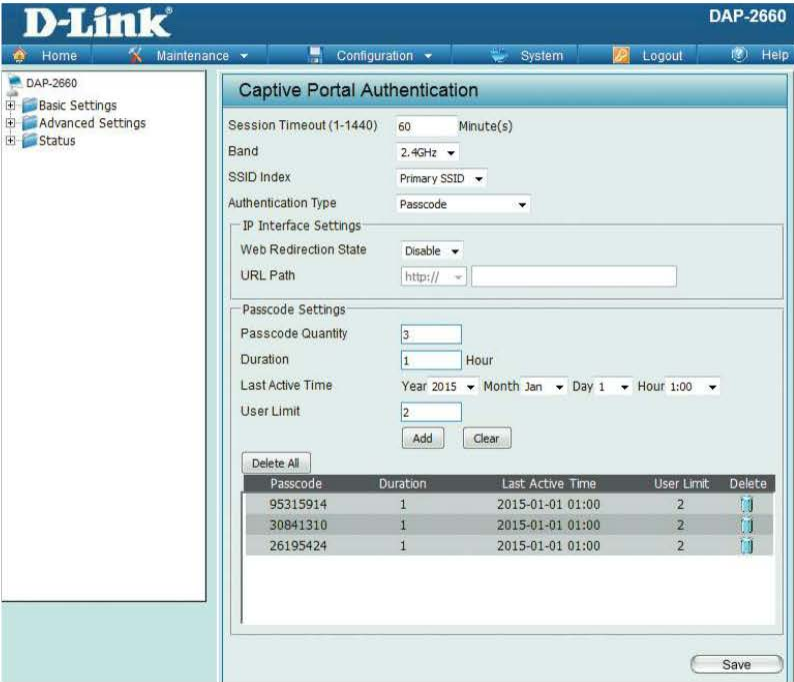


Рис. 8.61. Настройка Captive portal на точке доступа D-Link DAP-2660

8.10.2. Виртуальные частные сети (VPN)

Для безопасного подключения к локальным сетям удаленных беспроводных клиентов используются технологии *виртуальных частных сетей (Virtual Private Network, VPN)*.

С помощью VPN, например, сотрудники компании, находящиеся за пределами корпоративной сети (в аэропорту, отеле или дома), могут получить безопасный доступ к файлам, приложениям или другим ресурсам офисной сети, используя публичные или домашние сети Wi-Fi. Домашние пользователи также могут создавать свои VPN-сети для безопасного доступа к ресурсам домашней сети извне.

VPN — это набор технологий, которые позволяют создавать логические сети, используя сети других сетевых протоколов в качестве транспортных (рис. 8.62).

При этом характеристики безопасности созданной логической сети могут отличаться от характеристик безопасности транспортной сети. VPN-подключения могут создаваться на различных уровнях модели OSI. Существует множество различных VPN-протоколов, но не все они обеспечивают целостность и конфиденциальность соединений.

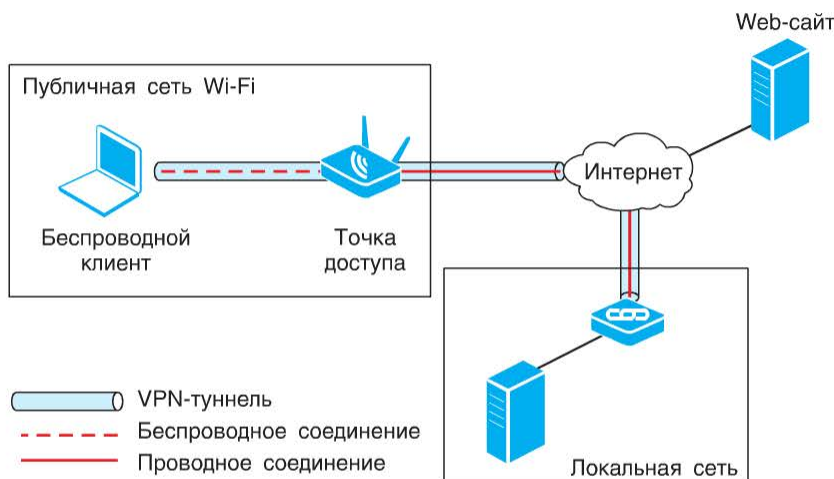


Рис. 8.62. VPN-подключение удаленного беспроводного клиента к локальной сети

8.10.3 Защита от вторжений

Одной из задач обеспечения безопасности больших беспроводных сетей является предотвращение установки несанкционированных точек доступа, появляющихся в сети как по вине персонала компании, так и в результате спланированной атаки злоумышленников. В любом случае наличие таких точек доступа представляет угрозу безопасности всей сети. Существуют различные способы подключения несанкционированных точек доступа, поэтому одной из задач сетевого администратора является мониторинг беспроводной сети с целью обнаружения несанкционированных устройств.

Для обнаружения несанкционированных точек доступа можно использовать анализаторы беспроводного трафика, такие как inSSIDer. Обходя с ноутбуком помещение и захватывая с помощью анализатора трафик беспроводной сети, можно получить информацию о точках доступа, установленных в зоне ее действия.

Точки доступа D-Link, поддерживающие функцию *Wireless Intrusion Protection*, позволяют обнаружить все точки доступа, находящиеся в радиусе их действия. Для просмотра списков обнаруженных устройств администратор должен заходить на Web-интерфейс каждой точки доступа. Это весьма трудозатратно, особенно в сети с большим количеством точек доступа. Обнаруженные точки можно маркировать как Valid (действительные), Neighborhood (соседние) и Rogue (несанкционированные) (рис. 8.63).

Наиболее удобным методом обнаружения несанкционированных точек доступа является использование центральной консоли, подключаясь к которой администратор может выполнять мониторинг всей сети. Возможность централизованного мониторинга предоставляют беспроводные контроллеры D-Link, которые поддерживают функцию *Wireless Intrusion Detection System*

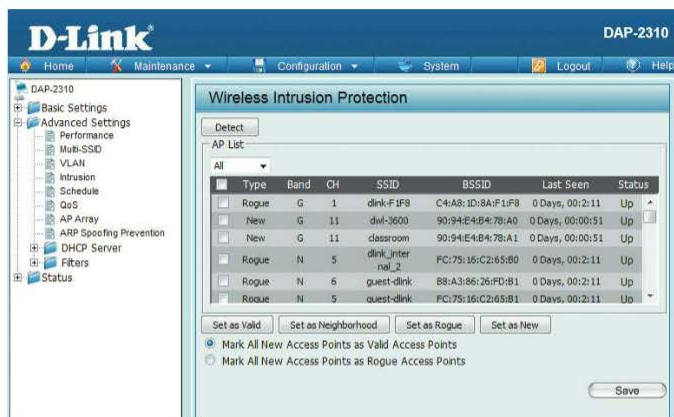


Рис. 8.63. Результат работы функции Wireless Intrusion Protection

(WIDS), предназначенную для обнаружения несанкционированных точек доступа и несанкционированных клиентов, а также различных угроз безопасности беспроводной сети.

Контроллер классифицирует обнаруженные точки по четырем группам: управляемая, автономная, неизвестная и несанкционированная. Управляемые точки доступа являются санкционированными устройствами, управляемыми контроллером. Автономные точки доступа — это санкционированные устройства, не управляемые с помощью контроллера (т. е. работающие автономно), но известные ему. Управляемые точки доступа выполняют радиочастотное сканирование и сообщают контроллеру о любой обнаруженной подозрительной точке доступа. Функция WIDS на контроллере определяет, что обнаруженная точка доступа является несанкционированной на основе различных параметров: используется неверный SSID, номер канала, неверные политики безопасности, неразрешенная конфигурация автономной точки доступа и пр. (рис. 8.64, 8.65).

Контроллеры используют инструменты визуализации, с помощью которых можно определить примерное местоположение несанкционированного устройства и показать его на плане помещения, если он предварительно подготовлен и загружен на контроллер (рис. 8.66).

С помощью контроллера можно также обнаруживать несанкционированных беспроводных клиентов и предотвращать подключение легальных клиентов к несанкционированным точкам доступа. Контроллер классифицирует беспроводных клиентов по трем группам: аутентифицированный, из черного списка, несанкционированный. Беспроводной клиент определяется контроллером как несанкционированный на основе различных параметров: его нет в базе данных пользователей, при его аутентификации возникает множество ошибок, пытается ассоциироваться с неизвестной точкой доступа и т. п. (рис. 8.67).

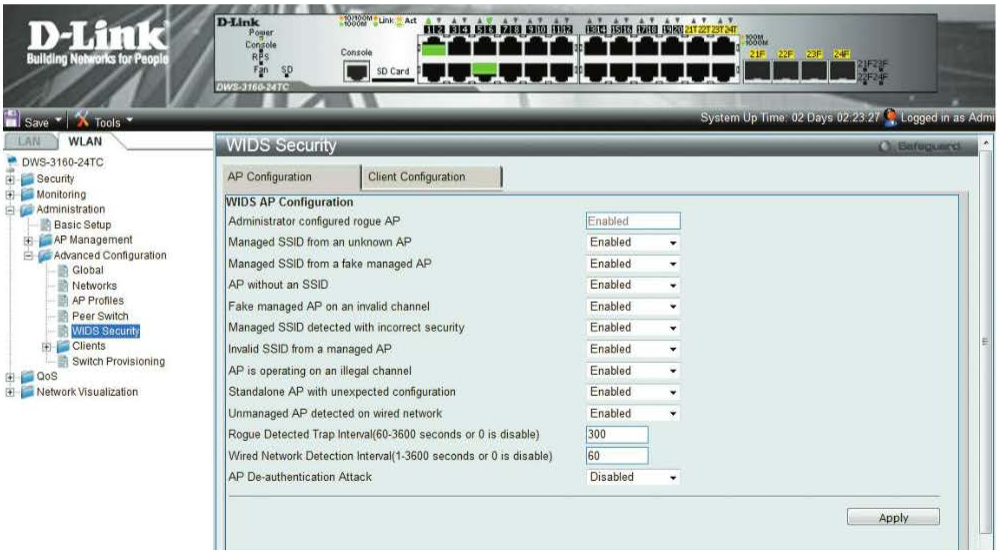


Рис. 8.64. Настройка параметров WIDS для определения несанкционированных точек доступа

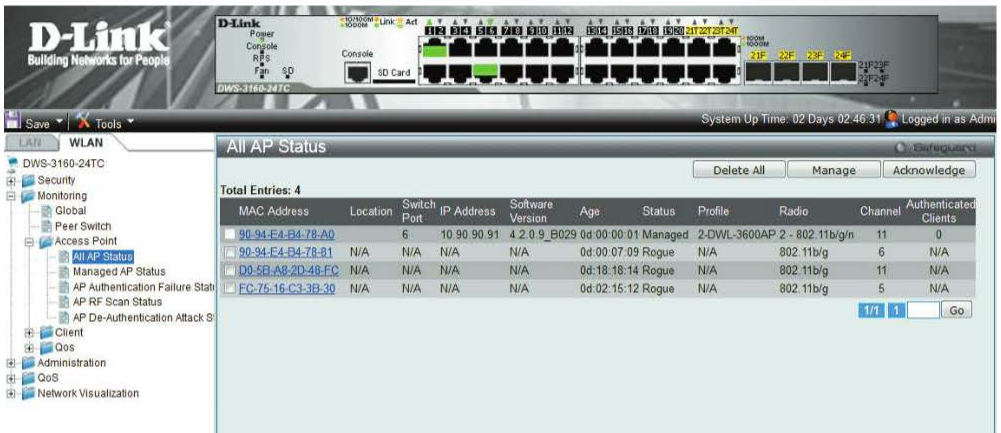


Рис. 8.65. Статус точек доступа

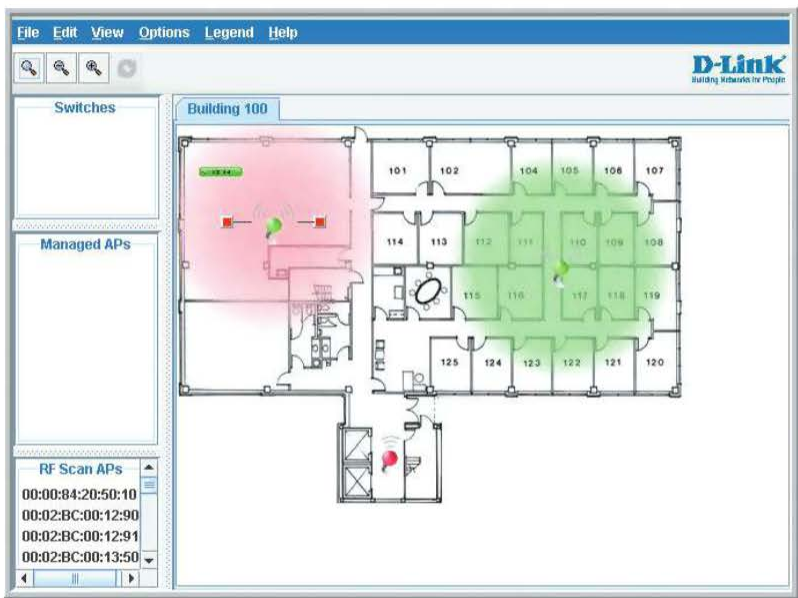


Рис. 8.66. Визуализация расположения несанкционированной точки доступа с помощью контроллера

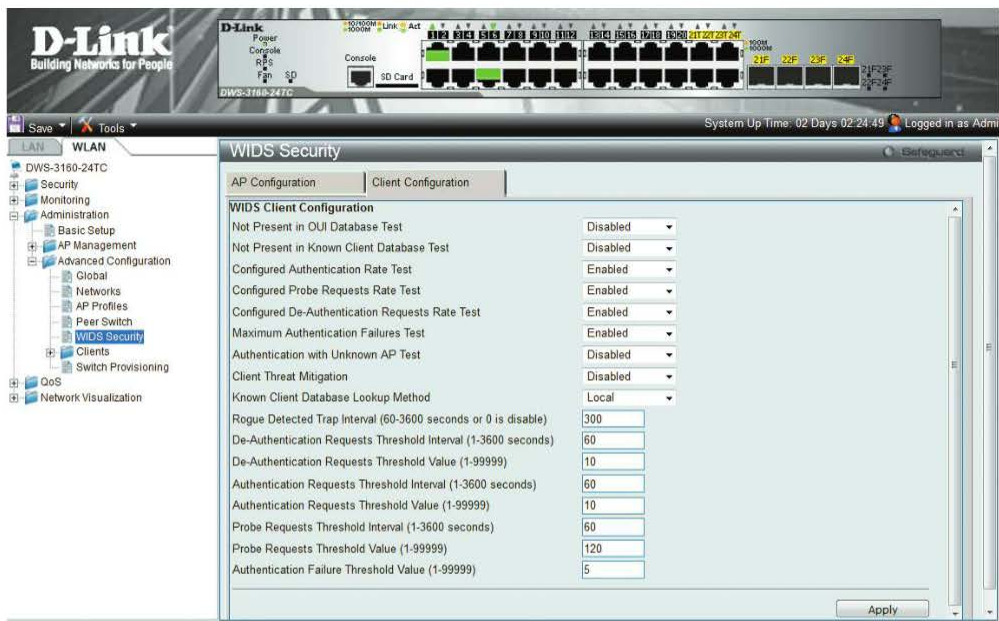


Рис. 8.67. Настройка параметров WIDS для определения несанкционированных клиентов

Для предотвращения подключения авторизованных клиентов к несанкционированным точкам доступа контроллер отправляет ложные сообщения отмены аутентификации, которые приводят к разрыву ассоциации клиентов с этими точками доступа.

8.11. Роуминг

Для покрытия беспроводной сетью небольшой территории, например квартиры или части офисного помещения, достаточно одной точки доступа или беспроводного маршрутизатора. Для покрытия больших территорий (этаж офисного помещения, складское помещение, гостиница и т. п.) используется несколько точек доступа или беспроводных маршрутизаторов, соединенных между собой в единую сеть. Одним из требований к беспроводной сети, покрывающей большую территорию, является обеспечение *роуминга*, т. е. возможности подключения клиентов к разным точкам доступа при их перемещении в пространстве.

Роуминг может выполняться на канальном (L2-роуминг) и сетевом (L3-роуминг) уровнях модели OSI. На канальном уровне клиент автоматически переключается между точками доступа по мере передвижения по территории. Дополнительно к этому клиент может переключаться между подсетями беспроводной сети (L3-роуминг).

Самый простой и широко распространенный алгоритм роуминга заключается в следующем: беспроводной клиент сохраняет связь с точкой доступа, с которой он ассоциирован, до момента, пока уровень сигнала не упадет ниже допустимого значения. После этого клиент переключается на новую точку доступа с максимальным уровнем сигнала. Для обеспечения возможности этого переключения необходимо, чтобы все точки доступа сети были настроены с одинаковыми SSID и параметрами безопасности (рис. 8.68).

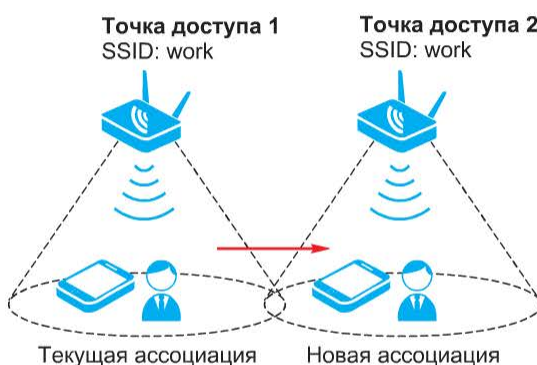


Рис. 8.68. Процесс роуминга

При переключении клиента на новую точку доступа он должен аутентифицироваться и ассоциироваться с ней. В случае использования автономных точек доступа или беспроводных маршрутизаторов каждое устройство рабо-

тает независимо друг от друга и процесс аутентификации/ассоциации должен выполняться каждый раз при переключении клиента на новое устройство. При этом моменту переключения на новую точку предшествует период существенного снижения скорости, потери пакетов и длительного времени ожидания. Кроме того, возможен обрыв соединения, что недопустимо, например, при просмотре видео или телефонном разговоре.

Для ускорения процесса переключения требуется заставить клиента переключиться на другую точку с лучшим уровнем сигнала, не дожидаясь, пока он примет такое решение самостоятельно. Некоторые модели точек доступа D-Link серии DAP-xxx поддерживают настройку порогового уровня сигнала клиентского устройства (RSSI Threshold), и если уровень сигнала от клиента оказывается ниже порогового, происходит принудительное отключение клиента от этой точки, и он вынужден подключиться к другой. Такое решение, однако, имеет следующий недостаток: если точка доступа находится на границе сети и клиент обнаруживает только ее, то при уровне сигнала ниже порогового он не сможет к ней подключиться и соединение с сетью будет потеряно.

Для ускорения процесса переключения между точками доступа в 2008 году выпущено дополнение к стандарту IEEE 802.11, получившее название IEEE 802.11r или Fast BSS Transition (FT), которое в настоящее время является частью стандарта IEEE 802.11–2012. Fast BSS Transition определяет методы установки параметров безопасности и QoS до ассоциации клиента с новой точкой доступа, что позволяет ему быстро переключаться между точками доступа без потери соединения. Ключи шифрования, которые были сгенерированы при подключении клиента к первой точке доступа, используются при аутентификации клиента с последующими точками доступа сети, что позволяет ему не выполнять полный процесс аутентификации.

Процесс роуминга при использовании Fast BSS Transition происходит следующим образом: клиент самостоятельно оценивает качество сигнала до точки доступа, с которой он ассоциирован, и до других окружающих его точек; как только клиент определяет, что уровень сигнала до точки доступа, с которой он ассоциирован, упал ниже некоторого уровня, он запускает процедуру переключения на другую точку. В случае если клиент обнаруживает точку доступа с лучшим уровнем сигнала, он отправляет ей запрос *повторной ассоциации* (*reassociation*). Новая точка доступа связывается со старой для проверки возможности роуминга клиента и возвращает клиенту ответ на запрос повторной ассоциации. Если ответ положительный, клиент переключается на новую точку доступа, которая получает ключи шифрования клиента у старой, уведомляет ее о том, что клиент переключился, и запрашивает данные, буферизированные для клиента. Старая точка доступа пересылает новой буферизированные данные, которые та, в свою очередь, передает клиенту. Обмен сообщениями между точками доступа может выполняться через проводную (DS) или беспроводную распределительную систему (WDS).

Несмотря на то что дополнение IEEE 802.11r к стандарту появилось в 2008 году, в настоящее время его поддерживают не все производители обо-

рудования. Для того чтобы клиент без поддержки 802.11r всегда мог подключаться к точке доступа или маршрутизатору с максимальным уровнем сигнала, компания D-Link разработала *технология интеллектуального распределения Wi-Fi-клиентов*, позволяющую точкам доступа или беспроводным маршрутизаторам беспроводной сети следить за уровнем сигнала подключенных к ним клиентов и разрывать с ними ассоциацию, если уровень сигнала от этих клиентов до соседних устройств выше. Благодаря этому в сети сокращается количество клиентов, передающих данные на низкой скорости (из-за низкого уровня сигнала) и тем самым снижающих общую пропускную способность сети. Для отслеживания уровня сигнала от клиентов точки доступа обмениваются между собой служебной информацией. Если клиент находится на границе сети (в зоне действия только одной точки доступа), то точка доступа не отключает клиента, потому что не получает информацию о нем от других точек доступа этой сети.

Функция интеллектуального распределения Wi-Fi-клиентов работает следующим образом (рис. 8.69):

- 1) каждая точка доступа хранит список ассоциированных с ней клиентов, а также информацию о клиентах, обнаруженных в зоне ее действия;
- 2) при падении уровня сигнала одного из клиентов ниже порогового значения точка доступа опрашивает все другие точки локальной сети: «видят» ли они данного клиента в зоне своего действия;
- 3) точки доступа, получившие запрос, отправляют ответ, содержащий информацию об уровне сигнала до этого клиента;
- 4) точка доступа, инициировавшая опрос, собирает информацию об уровне сигнала до клиента от соседних точек;
- 5) если уровень сигнала, обеспечиваемый другой точкой доступа, больше порогового значения на заранее определенную величину, то текущая точка доступа отключает клиента, отправляя ему сообщение о разрыве ассоциации;

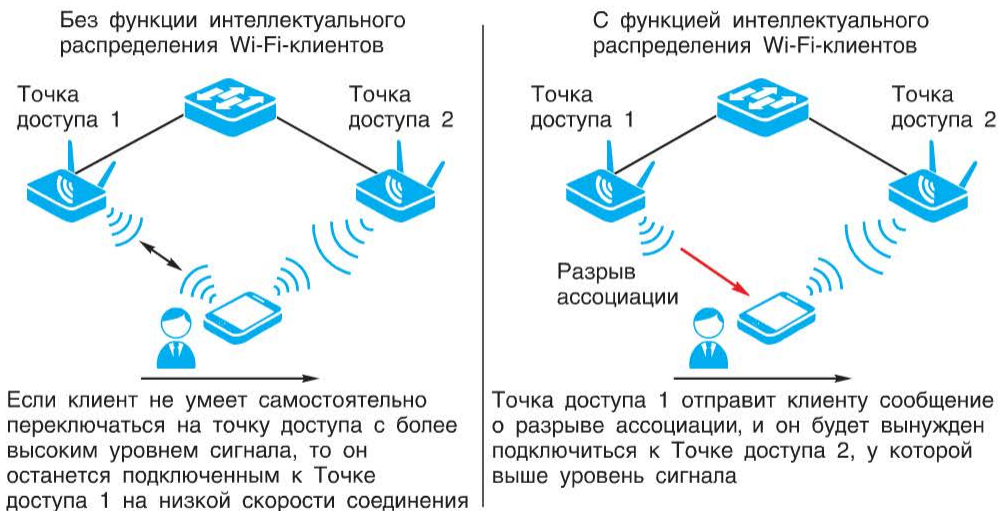


Рис. 8.69. Функция интеллектуального распределения Wi-Fi-клиентов

6) клиент, потеряв ассоциацию с текущей точкой доступа, пытается подключиться к сети и ассоциируется с новой точкой с наилучшим уровнем сигнала;

7) в случае если уровень сигнала от текущей точки доступа до клиента оказывается выше, чем от соседней, процесс отключения не выполняется.

Функция интеллектуального распределения Wi-Fi-клиентов предназначена для использования в домашних сетях и сетях небольших офисов (рис. 8.70). Точки доступа или беспроводные маршрутизаторы с поддержкой этой функции могут находиться как в одной, так и в разных IP-подсетях. Если беспроводная сеть не разбита на IP-подсети, рекомендуется использовать не более восьми точек доступа или маршрутизаторов, поскольку обмен служебной информацией между ними выполняется с использованием широковещательных сообщений. При разбиении беспроводной сети на IP-подсети точки доступа и маршрутизаторы обмениваются информацией с помощью многоадресных сообщений и их количество в объединенной сети может достигать 16.

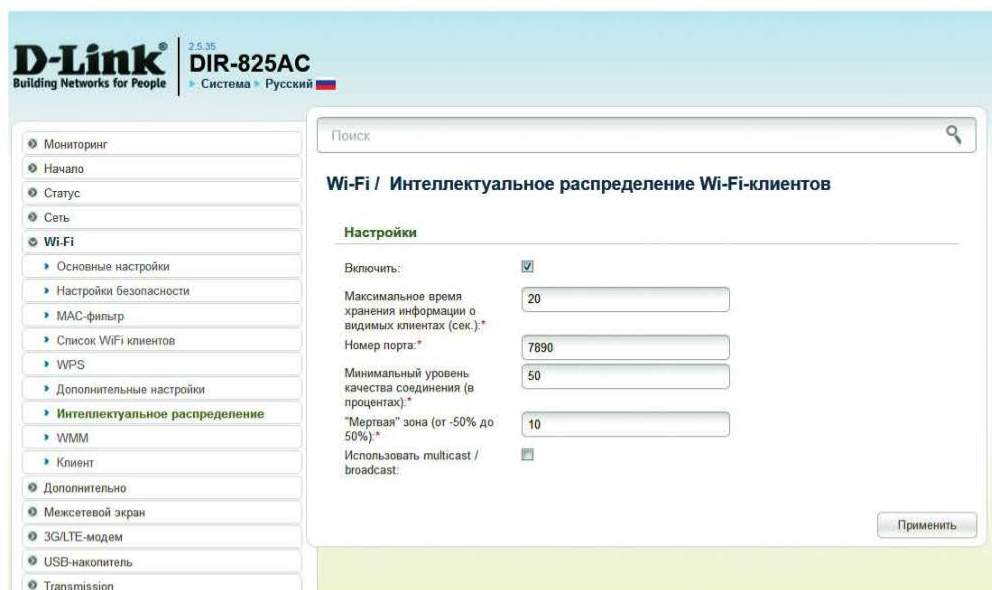


Рис. 8.70. Настройка функции интеллектуального распределения Wi-Fi-клиентов

В средних и больших корпоративных сетях функцию роуминга можно эффективно организовать с помощью беспроводного контроллера, что обеспечивает наиболее быстрое переключение клиентов между точками доступа. Для этого все точки доступа сети должны быть настроены с одинаковыми SSID и параметрами безопасности. Роуминг может выполняться как между точками доступа, подключенными к одному контроллеру, так и между точками, подключенными к группе контроллеров, образующих кластер. Рассмотрим, как выполняется роуминг с использованием контроллера.

Клиент принимает решение о переключении с одной точки доступа на другую в ситуации, когда уровень сигнала точки, с которой он ассоциирован, падает ниже порогового значения. Клиент при этом отправляет запрос ассоциации на новую точку, которая обращается к контроллеру для получения от него ключей шифрования, сгенерированных при начальном подключении клиента к сети. Таким образом, процесс аутентификации и ассоциации с новой точкой доступа при использовании контроллера выполняется значительно быстрее, чем при использовании автономных точек доступа, поскольку не требуется затрат времени на генерацию новых ключей шифрования.

При использовании унифицированных точек доступа и контроллеров D-Link дополнительно к L2-роумингу можно организовать L3-роуминг, т. е. роуминг между различными IP-подсетями. Целью L3-роуминга является прозрачное перемещение клиента с сохранением его первоначального IP-адреса. При этом несмотря на то, что точки доступа находятся в разных IP-подсетях, клиент при перемещении между ними не меняет свой IP-адрес.

В беспроводных контроллерах D-Link могут использоваться следующие методы туннелирования, обеспечивающие поддержку L3-роуминга: распределенные L2-туннели (поддерживаются контроллерами DWC-1000/2000 и DWS-3160-xx), L3-туннели (поддерживаются только контроллерами DWS-3160-xx).

Режим распределенного L2-туннелирования (distributed tunnel)

Домашней точкой доступа называется та точка, с которой клиент ассоциировался изначально. При перемещении клиента в другую IP-подсеть и ассоциации с новой точкой доступа она, используя управляющий L2-туннель с контроллером (CAPWAP-туннель), возвращает домашней точке доступа весь трафик клиента (для передачи трафика внутри туннеля используется протокол UDP). Домашняя точка доступа отправляет весь трафик, полученный через туннель, в проводную сеть. Таким образом трафик возвращается к клиенту в обратном направлении. При перемещении клиента к другой точке доступа из его подсети новая точка становится для него домашней и туннель не создается.

Для работы роуминга на всех точках доступа, подключенных к одному или нескольким контроллерам беспроводной сети, должен быть активизирован режим распределенного L2-туннелирования.

Режим L3-туннелирования (L3-tunnel)

В этом режиме трафик беспроводных клиентов передается через L3-туннель: между точкой доступа и контроллером создается простой IP-IP-туннель без шифрования. Для работы роуминга все точки доступа должны иметь одинаковые настройки туннеля.

При подключении клиента к точке доступа весь его трафик, включая запросы на получение IP-адреса, передаются по L3-туннелю на контроллер. Далее контроллер отправляет этот трафик в проводную сеть. Таким образом, не важно, в какой именно IP-подсети расположена точка доступа. Контроллер хранит в таблице коммутации MAC-адреса устройств, подключенных

к туннелю, поэтому трафик клиента всегда будет доставлен в тот сегмент сети, к которому подключена требуемая точка доступа (рис. 8.71).

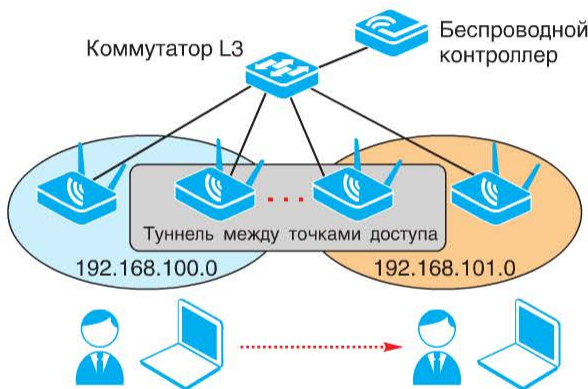


Рис. 8.71. Роуминг между подсетями

8.12. Функции настройки и управления

Каждая точка доступа требует выполнения с ней операций настройки, мониторинга и контроля. В больших беспроводных сетях число точек доступа обычно превышает 10, что требует от сетевого администратора значительных затрат времени на конфигурацию каждого отдельного устройства. Для повышения эффективности управления и мониторинга WLAN D-Link предлагает следующие решения: технологию AP Array, технологию кластеризации, программное обеспечение SNMP-управления D-View, централизованное управление точками доступа с помощью программных и аппаратных беспроводных контроллеров.

8.12.1. Технология AP Array

AP Array является средством централизованного управления группой автономных точек доступа, соединенных друг с другом через проводную сеть Ethernet. Эта функция встроена в программное обеспечение устройств и доступна для настройки через Web-интерфейс.

При использовании AP Array администратору требуется вручную настроить только одну точку доступа, после чего созданная конфигурация будет автоматически применена к остальным точкам доступа, входящим в группу. В группу AP Array может быть объединено до 32 точек доступа D-Link серии DAP-xxx, поддерживающих функцию AP Array 2.0 (предыдущая версия этой функции позволяла объединять в группу до восьми устройств). Количество самих групп не ограничено, но требуется, чтобы все группы в пределах одной IP-подсети имели разные имена. В группу могут быть объединены точки доступа разных моделей при условии, что они поддерживают функцию AP Array одинаковой версии.

Для включения точки доступа в группу AP Array в ее настройках требуется указать имя группы и пароль. Каждая точка доступа может быть членом только одной группы AP Array. Следует отметить, что в группу AP Array можно объединять только точки доступа в рамках одной IP-подсети.

Существует три роли, которые точка доступа может выполнять в группе AP Array (рис. 8.72):

- ведущая точка доступа (*Master*): управляет настройками всех членов группы. В каждой группе может быть только одна ведущая точка доступа;
- резервная ведущая точка доступа (*Backup Master*): выполняет функции ведущей точки доступа, если последняя выходит из строя. Каждая группа может иметь несколько резервных ведущих точек доступа;
- ведомая точка доступа (*Slave*): автоматически получает настройки от ведущей точки доступа.

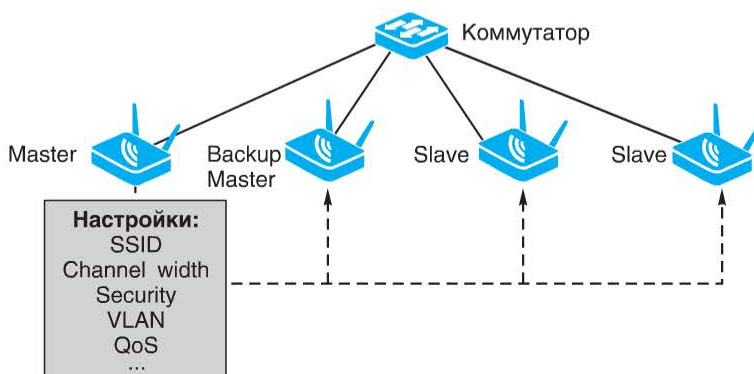


Рис. 8.72. Технология AP Array

Если в группу включены несколько ведущих точек доступа, то устройство, работающее в сети дольше всех, станет ведущей (*Master*) точкой, а включенные в группу позже — резервными (*Backup Master*) точками.

Ведущая точка доступа синхронизирует настройки со всеми ведомыми и резервными точками доступа всякий раз, когда в ее конфигурацию вносят изменения и нажимают в Web-интерфейсе кнопку «Save & Activate». При этом существует возможность выбора параметров, настройки которых будут применяться к резервным и ведомым точкам доступа (рис. 8.73). Остальные параметры при необходимости должны быть индивидуально настроены на каждой точке доступа, входящей в группу AP Array. Ведущая точка доступа отправляет сигнал проверки статуса ведомых точек доступа с интервалом 1 минута. Если какие-либо из них были настроены вручную, ведущая точка доступа автоматически синхронизирует их конфигурацию.

Если ведущая точка доступа выходит из строя, ее роль берет на себя резервная точка доступа. В том случае, если резервная точка доступа не была настроена и при этом в сети остались только ведомые точки доступа, они будут функционировать как обычные автономные точки доступа до тех пор, пока в сети снова не появится ведущая точка доступа.

Wireless Basic Settings <input checked="" type="checkbox"/>			
Network Name (SSID)	<input checked="" type="checkbox"/>	SSID Visibility	<input checked="" type="checkbox"/>
Auto Channel Selection	<input checked="" type="checkbox"/>	Channel Width	<input checked="" type="checkbox"/>
Security	<input checked="" type="checkbox"/>	Band	<input checked="" type="checkbox"/>
Wireless Advanced Setting <input checked="" type="checkbox"/>			
Data Rate	<input checked="" type="checkbox"/>	Beacon Interval	<input checked="" type="checkbox"/>
DTIM Interval	<input checked="" type="checkbox"/>	Transmit Power	<input checked="" type="checkbox"/>
WMM (Wi-Fi Multimedia)	<input checked="" type="checkbox"/>	Ack Time Out	<input checked="" type="checkbox"/>
Wireless ACL	<input checked="" type="checkbox"/>	Short GI	<input checked="" type="checkbox"/>
Link Integrity	<input checked="" type="checkbox"/>	Connection Limit	<input checked="" type="checkbox"/>
IGMP Snooping	<input checked="" type="checkbox"/>		
Multiple SSID & VLAN <input checked="" type="checkbox"/>			
SSID	<input checked="" type="checkbox"/>	SSID Visibility	<input checked="" type="checkbox"/>
Security	<input checked="" type="checkbox"/>	WMM	<input checked="" type="checkbox"/>
VLAN	<input checked="" type="checkbox"/>		
Advanced Functions <input checked="" type="checkbox"/>			
Schedule Settings	<input checked="" type="checkbox"/>	QoS Settings	<input checked="" type="checkbox"/>
Log Settings	<input checked="" type="checkbox"/>	Time and Date Settings	<input checked="" type="checkbox"/>
DHCP server Settings	<input checked="" type="checkbox"/>		
Administration Settings <input checked="" type="checkbox"/>			
System Name Settings	<input checked="" type="checkbox"/>	SNMP Settings	<input checked="" type="checkbox"/>
Login Settings	<input checked="" type="checkbox"/>	Console Settings	<input checked="" type="checkbox"/>

Рис. 8.73. Синхронизируемые параметры настройки в группе AP Array

Последовательность настройки управления по технологии AP Array:

- 1) одна из точек доступа группы настраивается в качестве ведущей (*Master*) (рис. 8.74): активизируется функция AP Array и устанавливается режим работы *Master*, задаются имя и пароль группы, выполняется настройка параметров точки доступа;
- 2) одна или несколько точек доступа группы настраиваются в качестве резервных ведущих (*Backup Master*): активизируется функция AP Array и устанавливается режим работы *Backup Master*, указываются имя и пароль группы, заданные на ведущей точке доступа;
- 3) одна или несколько точек доступа группы настраиваются в качестве ведомых (*Slave*): активизируется функция AP Array и устанавливается режим работы *Slave*, указываются имя и пароль группы, заданные на ведущей точке доступа.

После выполнения всех настроек резервные ведущие и ведомые точки доступа начинают автоматически синхронизировать свои параметры с ведущей.

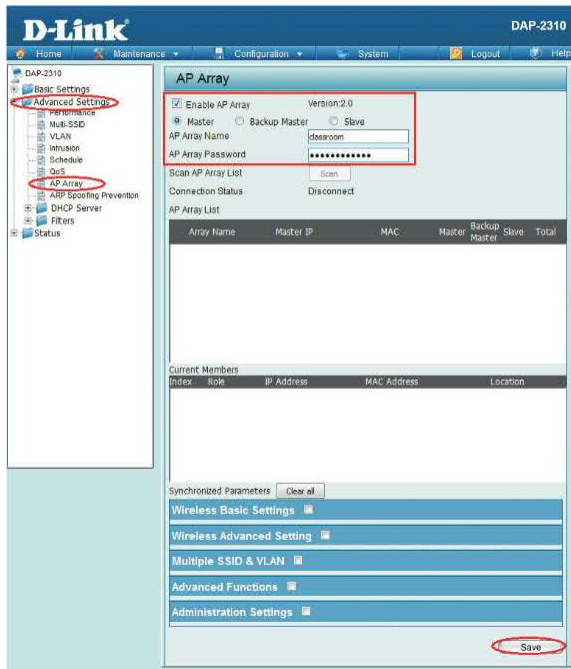


Рис. 8.74. Настройка точки доступа в качестве ведущей (Master)

При объединении точек доступа в группу AP Array можно не только централизованно управлять ими, но и выполнять балансировку нагрузки между ними на основе анализа использования полосы пропускания.

8.12.2. Технология кластеризации точек доступа

Централизованное управление группой унифицированных точек доступа D-Link серии DWL-xxx может выполняться с помощью технологии кластеризации или с использованием беспроводного контроллера.

Технология кластеризации позволяет централизованно управлять группой из восьми унифицированных точек доступа без использования беспроводного контроллера. В отличие от технологии AP Array все точки доступа, входящие в кластер, равноправны. После задания настроек на одной из них эти настройки автоматически применяются на всех остальных точках доступа кластера. Если в кластер добавляется точка доступа со своими отличными настройками, они будут синхронизированы с настройками кластера.

При объединении в кластер точки доступа могут быть соединены друг с другом как через проводную (DS), так и беспроводную распределительную систему (WDS).

Для формирования кластера из точек доступа должны быть выполнены следующие условия:

- 1) точки доступа должны быть одной модели;
- 2) точки доступа должны находиться в одном L2-сегменте сети (иметь одинаковый SSID) и в одной IP-подсети;
- 3) в настройках каждой из точек указано одинаковое название кластера;
- 4) функция кластеризации включена на всех точках доступа.

Настройка функции кластеризации выполняется единообразно на всех точках доступа, объединяемых в кластер:

1) в Web-интерфейсе точки выбирают вкладку *Cluster* → *Access Points*. В поле *Location* указывают место нахождения точки доступа (например, room1), в поле *Cluster name* имя кластера (например, cluster1) и нажимают кнопку *Apply* для сохранения настроек (рис. 8.75).



Рис. 8.75. Добавление точки доступа в кластер

Поля *Location* и *Cluster name* нужно настроить на каждой точке, которая будет входить в кластер. При этом значение поля *Cluster name* у всех точек доступа должно быть одинаковым, а описание местонахождения точек (поле *Location*) может отличаться;

2) после настройки параметров *Location* и *Cluster name* на каждой из точек доступа нажимают кнопку *Start Clustering*;



Рис. 8.76. Информация о точках доступа, входящих в кластер

3) после настройки кластеризации на вкладке *Cluster* → *Access Points* любой из точек доступа отображается список устройств, входящих в кластер (рис. 8.76). Если щелкнуть по IP-адресу любой точки доступа из списка, то будет выполнен переход в ее Web-интерфейс;

4) если требуется удалить точку доступа из кластера, необходимо зайти в ее Web-интерфейс и во вкладке *Cluster* → *Access Points* нажать кнопку *Stop Clustering*.

Для того чтобы узнать, к каким точкам кластера подключены клиенты, необходимо зайти на вкладку *Cluster* → *Sessions*.

8.12.3. Управление точками доступа с использованием аппаратного беспроводного контроллера

Для централизованного управления большим количеством унифицированных точек доступа наилучшим решением является использование аппаратного беспроводного контроллера. Аппаратные беспроводные контроллеры D-Link представлены моделями DWC-1000 и DWC-2000 и серией беспроводных коммутаторов DWS-3160-xx. Напомним, что у беспроводных коммутаторов функции беспроводного контроллера дополнены функциями коммутатора.

Существует несколько вариантов соединения беспроводного контроллера с точками доступа: непосредственное подключение, подключение через коммутатор и подключение через маршрутизатор. В зависимости от модели базовое программное обеспечение одного контроллера позволяет одновременно управлять 6 (DWC-1000), 12 (DWS-3160-xx) или 64 (DWC-2000) точками доступа. При установке дополнительных лицензий число управляемых точек доступа можно увеличить до 24 (DWC-1000), 48 (DWS-3160-xx) или 256 (DWC-2000).

Контроллеры могут быть объединены в кластер. Максимальное количество контроллеров в кластере может быть 4 или 8 (в зависимости от модели). Благодаря кластеризации упрощается управление беспроводной сетью, так как все настройки можно выполнять на одном контроллере, выполняющем роль ведущего (рис. 8.77). При выборе ведущего контроллера сравниваются приоритеты всех контроллеров, объединяемых в кластер, и среди них выбирается устройство с наивысшим. При равенстве приоритетов ведущим становится контроллер с меньшим значением IP-адреса. Контроллеры кластера обмениваются между собой информацией о подключенных точках доступа и позволяют организовать роуминг между ними.

Напомним основные функции контроллеров:

- администратор может централизованно задавать единую конфигурацию сразу для всех подключенных к контроллеру точек доступа вместо того, чтобы настраивать каждую их них в отдельности, а также обновлять их программное обеспечение;

- с помощью контроллера можно выполнять обнаружение несанкционированных точек доступа и клиентов, а также идентифицировать различные угрозы безопасности беспроводной сети с помощью функции *Wireless Intrusion Detection System* (WIDS);

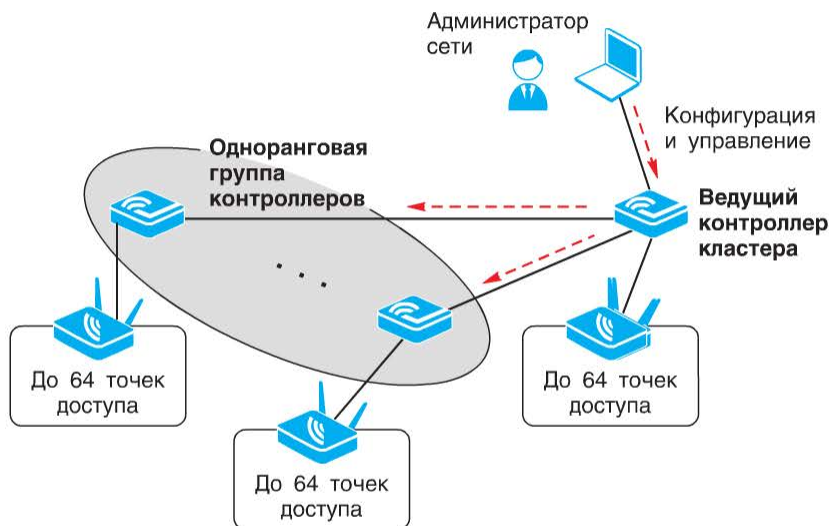


Рис. 8.77. Кластер контроллеров

- при подключении точек доступа к контроллеру он выполняет их аутентификацию и автоматическую настройку в соответствии с профилем конфигурации. Каждая точка доступа автоматически настраивается на оптимальный радиочастотный канал и выходную мощность передатчика, обеспечивая беспроводных клиентов сигналом наилучшего качества;

- с помощью контроллера можно эффективно организовать функцию роуминга на втором и третьем уровнях модели OSI;

- контроллер позволяет организовать гостевой доступ и отделить гостевой трафик от трафика внутренней сети;

- повышается отказоустойчивость сети благодаря поддержке функции резервирования контроллеров и механизма AP provisioning, позволяющего автоматически переключать управление точками доступа с вышедшего из строя контроллера на резервный;

- контроллер позволяет повысить производительность сети за счет возможности балансировки нагрузки между точками доступа и регулирования параметров радиочастотных каналов на основе анализа их текущего состояния;

- при использовании в сети беспроводного коммутатора DWS-3160-24PC можно организовать питание точек доступа по технологии Power over Ethernet, так как его порты Ethernet поддерживают стандарт IEEE 802.3at.

8.12.4. Программный контроллер D-Link Central WiFiManager

Central WiFiManager CWM-100 представляет собой программный контроллер для централизованного управления автономными точками доступа серии DAP-xxx в сетях малых, средних и крупных предприятий. С помощью CWM-100 администратор сети может управлять большим количеством точек доступа (до 1000), находясь как непосредственно в сети, так и за ее предела-

ми (удаленно). В отличие от аппаратных контроллеров CWM-100 не требует приобретения дополнительных лицензий для увеличения числа управляемых точек доступа при расширении сети (рис. 8.78).

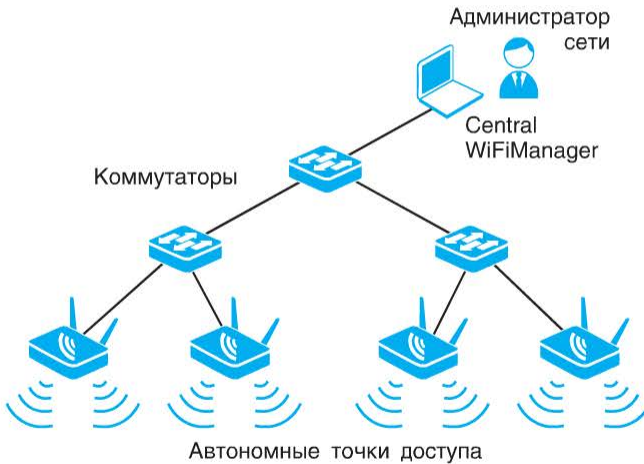


Рис. 8.78. Управление с помощью Central WiFiManager

Функции Central WiFiManager и AP Array являются взаимно исключающими. Автономная точка доступа может работать под управлением только одной из этих функций.

Программное обеспечение контроллера может быть установлено как на компьютер под управлением Microsoft Windows, так и на удаленную облачную платформу. ПО Central WiFiManager можно загрузить бесплатно с сайта компании D-Link (www.dlink.ru).

В решение Central WiFiManager входят следующие компоненты: сервер Central WiFiManager (CWM-сервер), модули управления точками доступа, утилита для обнаружения точек доступа.

Для развертывания решения необходимо установить CWM-сервер на компьютере под управлением ОС Windows с помощью мастера, затем запустить установку модулей управления точками доступа, находящимися в сети. Список точек доступа серии DAP-xxx, поддерживающих работу с Central WiFiManager, указан в описании контроллера на сайте компании D-Link. После завершения всех установок запустить работу Central WiFiManager Server с помощью значка на рабочем столе и нажать кнопку в виде треугольника в открывшемся окне (рис. 8.79).

Для управления точками доступа ПО Central WiFiManager использует Web-интерфейс, для доступа к которому нужно щелкнуть по значку Central WiFiManager на рабочем столе Windows. На открывшейся странице авторизации (рис. 8.80) ввести имя пользователя, пароль (по умолчанию имя пользователя — *admin*, пароль — *admin*) и код идентификации CAPTCHA

(с учетом регистра). Программный контроллер поддерживает возможность администрирования точек доступа несколькими пользователями с разным уровнем полномочий.

После авторизации можно начинать работу с Central WiFiManager. Для обнаружения и добавления точек доступа, которые будут управляться через контроллер, используется специальная утилита, входящая в комплект ПО Central WiFiManager.

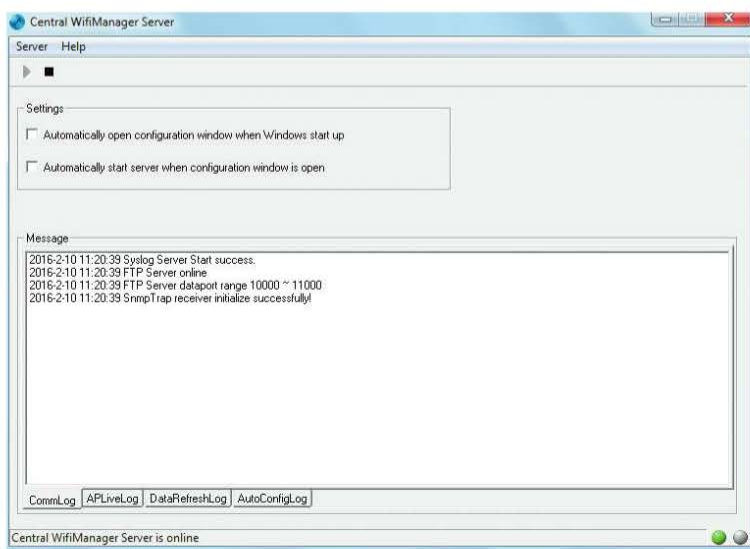


Рис. 8.79. Запуск Central WiFiManager Server

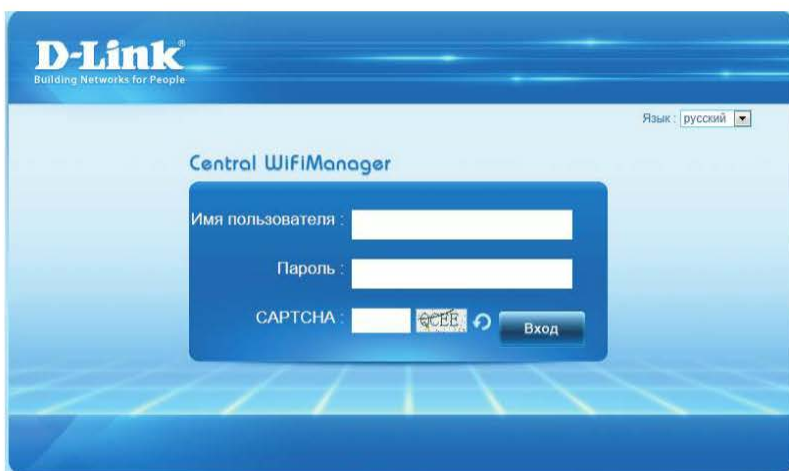


Рис. 8.80. Окно авторизации Central WiFiManager

Программный контроллер позволяет выполнять в беспроводной сети настройку следующих функций:

- аутентификацию пользователей с использованием локальной базы данных и внешних серверов RADIUS, LDAP, POP3;
- реализацию портала аутентификации пользователей хот-спота (публичной беспроводной сети);
- реализацию портала аутентификации при гостевом доступе;
- автоматическое управление выходной мощностью точек доступа;
- автоматический выбор канала точками доступа;
- самовосстановление зоны покрытия в результате выхода из строя точки доступа за счет увеличения мощности соседних;
- балансировку нагрузки между диапазонами двухдиапазонных точек доступа;
- обнаружение несанкционированных точек доступа.

Лабораторные работы по курсу «Технологии современных беспроводных сетей Wi-Fi»

Рекомендации по организации лабораторных работ

Практическая часть курса «Технологии современных беспроводных сетей Wi-Fi» состоит из 13 лабораторных работ, среди которых 11 базовых и 2 факультативных.

Для выполнения лабораторных работ группой учащихся, состоящей из 10 человек, рекомендуется следующий комплект оборудования:

- Точка доступа DAP-2310 9 шт.
- Коммутатор DES-1100-16 6 шт.
- Беспроводной адаптер DWA-160 или DWA-582 12 шт.
- Антенна ANT24-0502 4 шт.
- Рабочая станция 12 шт.
- Ноутбук 4 шт.
- Кабель Ethernet 15 шт.

Дополнительно для факультативных лабораторных работ:

- Точка доступа DAP-2660 3 шт.
- Беспроводной адаптер DWA-182 3 шт.

Каждая лабораторная работа содержит общую схему сети с указанием количества рабочих мест, на которое она рассчитана.

Во избежание значительной интерференции при выполнении лабораторных работ требуется ограничить радиус действия каждой точки доступа 1...2 м. Для этого в начале каждой лабораторной работы необходимо установить значение мощности передатчика точки доступа равное 12,5 %.

Для выполнения работ из учащихся организуются рабочие группы, каждой из которых присваивается номер (N). Адреса рабочих станций назначаются в зависимости от номера группы, таким образом каждая группа будет находиться в отдельной подсети. Например, IP-адрес рабочей станции 192.168.N.1 с маской подсети 255.255.255.0, где N — номер рабочей группы. Номер рабочей группы будет также использоваться при назначении имени беспроводной сети (SSID).

Внимание: при подключении к беспроводным сетям в интерфейсе настройки Windows снимайте галочку «Подключаться автоматически».

Все примеры настройки в лабораторных работах приведены для рабочей группы с номером 0.

Настройка устройств в лабораторных работах приведена для следующих версий программного обеспечения:

- Точка доступа DAP-2310 — ПО версии 1.16 или выше;
- Точка доступа DAP-2660 — ПО версии 1.11 или выше;
- Коммутатор DES-1100-16 — ПО версии 1.00.11 или выше.

Для проведения лабораторных работ требуется следующее дополнительное программное обеспечение (ПО):

- программа мониторинга беспроводных сетей *inSSIDer Home* (<http://www.techspot.com/downloads/5936-inssider.html>);
- анализатор трафика *Microsoft Network Monitor* (<https://www.microsoft.com/en-us/download/details.aspx?id=4865>);
- программный контроллер для централизованного управления точками доступа *D-Link Central WiFiManager* (http://www.dlink.ru/ru/products/2/2086_d.html);
- утилита командной строки для анализа пропускной способности сети *iPerf* (<https://iperf.fr/iperf-download.php#windows>).

Лабораторная работа № 1. Преобразование единиц измерения в беспроводных сетях

При расчете различных параметров беспроводных сетей зачастую приходится выполнять преобразование одних единиц измерения в другие. В технических описаниях и законодательных актах, регулирующих использование радиочастотного спектра в России, присутствуют как линейные (ватты, Вт), так и логарифмические (децибелы, дБ) единицы измерения.

Децибел (русское обозначение дБ, международное dB) — доляная единица, равная 0,1 Б; логарифмическая единица (т. е. безразмерная относительная величина), предназначенная для измерения отношения двух одноименных величин (например, уровней мощности, затухания и усиления сигналов) с применением к полученному отношению логарифмического масштаба. В децибелах принято измерять затухание волн при распространении их в поглощающей среде, коэффициент усиления антенны, отношение сигнал/шум.

Для оценки, например, мощности сигнала, выраженной в дБ, необходимо вычислить соотношение

$$P_{dB} = 10 \lg \frac{P_1}{P_0}, \quad (Л1.1)$$

где P_1 — измеренная мощность; P_0 — мощность, принятая за основу.

В отличие от безразмерного децибела для выражения абсолютных значений мощности используются величины dBm (дБм) и dBW (дБВт). Для их использования необходимо условиться, какой уровень измеряемой физической величины будет принят за базовый (условный 0 дБ).

В dBm (дБм) обычно выражается мощность передатчика. За нулевой уровень дБм принята мощность 1 мВт. Для перевода мощности из мВт в дБм необходимо выполнить следующее вычисление:

$$P_{dBm} = 10 \lg \frac{P_{mW}}{1mW}, \quad (Л1.2)$$

где P_{dBm} — мощность передатчика, выраженная в дБм; P_{mW} — мощность передатчика, выраженная в мВт.

Обратное преобразование из дБм в мВт выполняется по формуле

$$P_{mW} = 10^{\frac{P_{dBm}}{10}}.$$

(Л1.3)

В dBW (дБВт) за нулевой уровень принята мощность 1 Вт. Формулы для перевода аналогичны вышеприведенным с той разницей, что в качестве нулевого уровня выбрана величина 1 Вт, а измеренная мощность также должна выражаться в ваттах.

Величина dBi (дБи) называется «изотропный децибел» (децибел относительно изотропного излучателя) и характеризует коэффициент усиления антенны относительно коэффициента направленного действия изотропного излучателя. Как правило, если не оговорено специально, характеристики усиления реальных антенн даются именно относительно усиления изотропного излучателя.

Децибелы являются нелинейными единицами измерения. Поэтому, когда говорят, например, об удвоении мощности, равной 100 мВт (20 дБм), это не означает, что мощность увеличилась до 40 дБм. 40 дБм соответствует 10 000 мВт. Увеличение мощности (в мВт) в 2 раза эквивалентно прибавлению к мощности (в дБм) 3 дБм. Уменьшение мощности в мВт в 2 раза эквивалентно вычитанию из мощности в дБм 3 дБм. Следовательно, при увеличении мощности 100 мВт в 2 раза, необходимо сложить 20 дБм и 3 дБм и получим мощность 23 дБм.

Цель работы: научиться переводить одни единицы измерения в другие.

ЗАДАНИЕ 1. Укажите значения дБм для каждого из следующих уровней мощности, выраженных в мВт. За нулевой уровень дБм примите мощность в 1 мВт. Округлите полученное значение до целого числа.

Мощность передатчика, мВт	Мощность передатчика, дБм
97	20
15	
37	
63	
420	
160	
1,6	
250	
900	
2	

РЕШЕНИЕ: для выполнения задания подставьте значение мощности передатчика в мВт в формулу (1.2). Например,

$$10 \lg \frac{97}{1} = 20 \text{ дБм.}$$

ЗАДАНИЕ 2. Укажите значения мВт для каждого из следующих уровней мощности, выраженных в дБм. Округлите полученное значение до целого числа.

Мощность передатчика, дБм	Мощность передатчика, мВт
16	40
30	
2	
40	
36	
33	
0	
28	
9	
31	

Решение: для выполнения задания подставьте значение мощности передатчика в дБм в формулу (1.3). Например,

$$10^{\frac{16}{10}} = 40 \text{ мВт.}$$

ЗАДАНИЕ 3

1. Мощность передатчика 200 мВт уменьшилась в 4 раза. Вычислите новое значение мощности и выразите его в дБм _____.

Решение: $P_1 = 0,25 P_0$. Подставим эти значения в формулу (1.1):

$$10 \lg 0,25 = -6 \text{ дБм.}$$

Значение мощности 200 мВт эквивалентно 23 дБм. Соответственно 23 дБм – 6 дБм = 17 дБм.

2. Мощность передатчика 63 мВт увеличилась в 32 раза. Вычислите новое значение мощности и выразите его в дБм _____.

3. Мощность передатчика 10 мВт уменьшилась в 10 раз. Вычислите новое значение мощности и выразите его в дБм _____.

4. Мощность передатчика 158 мВт уменьшилась в 5 раз. Вычислите новое значение мощности и выразите его в дБм _____.

5. Мощность передатчика 1000 мВт уменьшилась в 10 раз. Вычислите новое значение мощности и выразите его в дБм _____.

6. Мощность передатчика 200 мВт увеличилась в 6 раз. Вычислите новое значение мощности и выразите его в дБм _____.
7. Мощность передатчика 40 дБм уменьшилась в 100 раз. Вычислите новое значение мощности и выразите его в дБм _____.
8. Мощность передатчика 30 дБм уменьшилась в 1000 раз. Вычислите новое значение мощности и выразите его в дБм _____.
9. Мощность передатчика 20 дБм уменьшилась в 2 раза. Вычислите новое значение мощности и выразите его в дБм _____.
10. Мощность передатчика 16 дБм увеличилась в 4 раза. Вычислите новое значение мощности и выразите его в дБм _____.

Лабораторная работа № 2. Создание беспроводной сети в инфраструктурном режиме

Основным строительным блоком беспроводной сети IEEE 802.11 является базовый набор услуг (*Basic Service Set, BSS*), который состоит из нескольких станций, реализующих общий протокол MAC и состоящих за доступ к разделяемой среде передачи. BSS может быть изолирован или соединен с магистральной распределительной системой (*Distribution System*) через точку доступа (*Access Point*).

Передача данных между клиентскими станциями выполняется через точку доступа независимо от того, находятся станция-отправитель и станция-получатель в одном или разных BSS. При передаче кадров от одной станции к другой в пределах одного BSS станция-отправитель сначала пересылает кадры точке доступа, которая затем направляет кадры нужному адресату. Если станция-получатель находится в другом BSS, станция-отправитель посылает кадры точке доступа, которая перенаправляет их через распределительную систему в направлении станции-получателя. Распределительная система может быть представлена как проводной, так и беспроводной сетью. Режим работы BSS, при котором все операции выполняются через точку доступа, называется инфраструктурным (*Infrastructure*).

Для подключения к проводному сегменту у точки доступа имеется сетевой интерфейс Ethernet с разъемом RJ-45 (*uplink port*). Через этот же интерфейс может осуществляться и настройка точки доступа. Точки доступа могут работать как в одном 2,4 или 5 ГГц, так и в обоих диапазонах частот (*dual-mode*). При этом работа в разных частотных диапазонах может осуществляться параллельно (*concurrent dual-mode*), если точкой доступа поддерживается такая функциональность.

В программном обеспечении точек доступа может быть реализована поддержка работы в следующих режимах: Access Point, WDS with AP, WDS, Wireless Client, AP Repeater.

В зависимости от того, какой режим выбран, точка доступа будет выполнять в сети разные функции.

Основным режимом работы точки доступа является Access Point. В этом режиме она выполняет свою непосредственную функцию: служит для создания беспроводной сети.

Режим беспроводного клиента (*Wireless Client*) используется в случае необходимости подключения к беспроводной сети одного устройства, не имеющего беспроводного интерфейса и разъема для установки беспроводного адаптера.

Режимы WDS и WDS with AP описаны и рассмотрены в лабораторной работе № 9.

Для расширения зоны покрытия можно использовать точку доступа, настроенную для работы в режиме повторителя (*Repeater*).

Для мониторинга беспроводных сетей в данной лабораторной работе используется бесплатная программа *inSSIDer Home*. С ее помощью можно посмотреть список беспроводных сетей, в зоне действия которых находится беспроводное устройство, узнать уровень сигнала, MAC-адрес точки доступа, используемые каналы и их загруженность, SSID, технологии обеспечения безопасности. На основе анализа уровня сигнала и загруженности частотных каналов осуществляется выбор наименее загруженного канала с максимальной скоростью и минимальными помехами.

Оборудование (на 2 рабочих места):

Рабочая станция	3 шт.
Беспроводной адаптер DWA-160 или DWA-582	2 шт.
Точка доступа DAP-2310	2 шт.
Кабель Ethernet	2 шт.
ПО — программа для мониторинга беспроводных сетей <i>inSSIDer Home</i> .	

Цель работы: научиться устанавливать беспроводной адаптер, изучить Web-интерфейс точки доступа DAP-2310 и режимы ее работы.

2.1. Установка драйвера беспроводного сетевого адаптера

Шаг 1. Запустите установку драйвера беспроводного адаптера DWA-160 и следуйте инструкциям мастера установки (рис. 2.1–2.3).

Примечание. Драйвер входит в комплект поставки оборудования. Также его можно бесплатно загрузить с сайта www.dlink.ru.

Шаг 2. Подключите адаптер DWA-160 к USB-порту рабочей станции и нажмите кнопку *Далее* (рис. 2.4, 2.5).

Шаг 3. После установки нажмите кнопку *Выход* (рис. 2.6).

При использовании адаптера DWA-582 подключите его к PCI-разъему рабочей станции, запустите драйвер и следуйте инструкциям мастера установки.



Рис. 2.1. Мастер установки

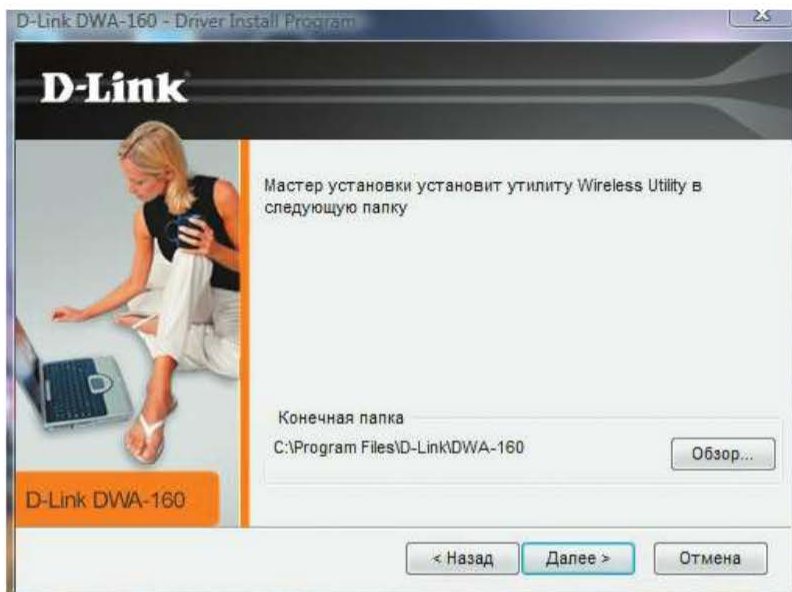


Рис. 2.2. Выбор папки установки драйвера



Рис. 2.3. Изменение названия папки

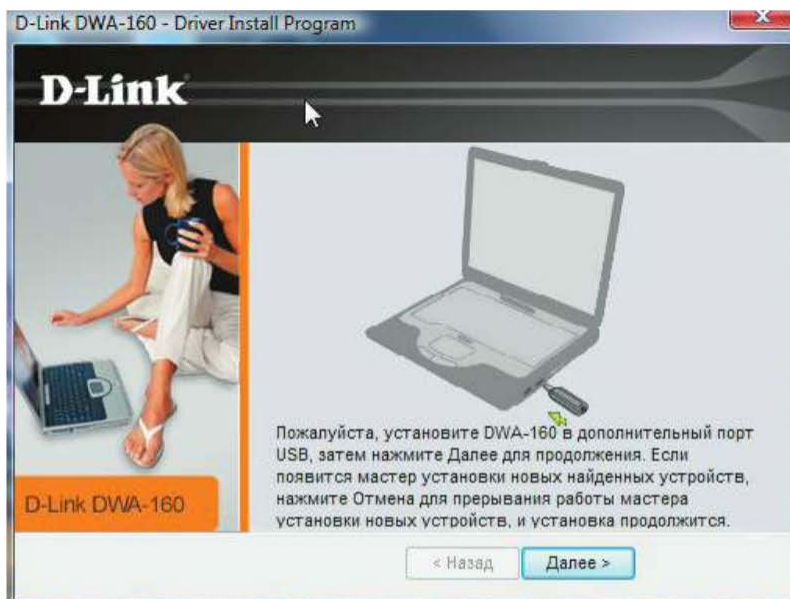


Рис. 2.4. Подключение адаптера к USB-порту

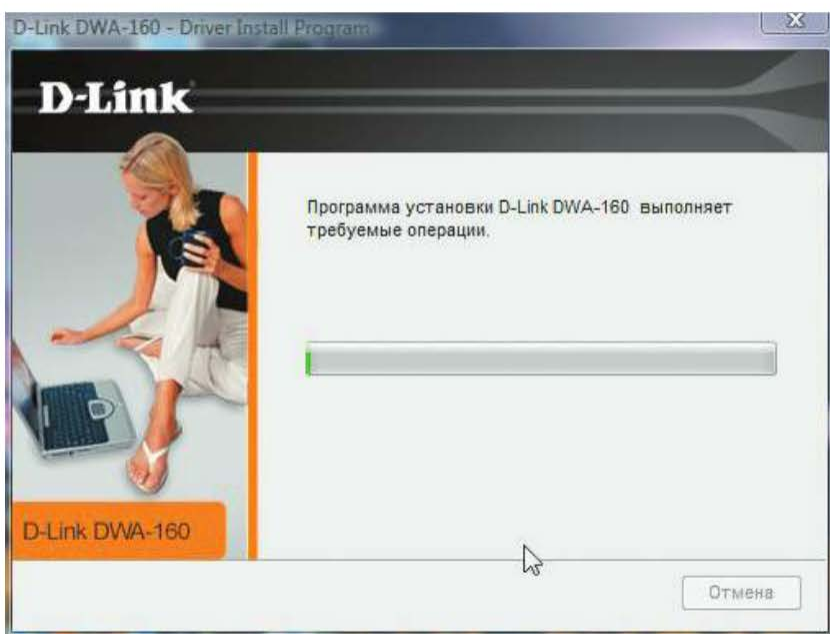


Рис. 2.5. Выполнение установки драйвера

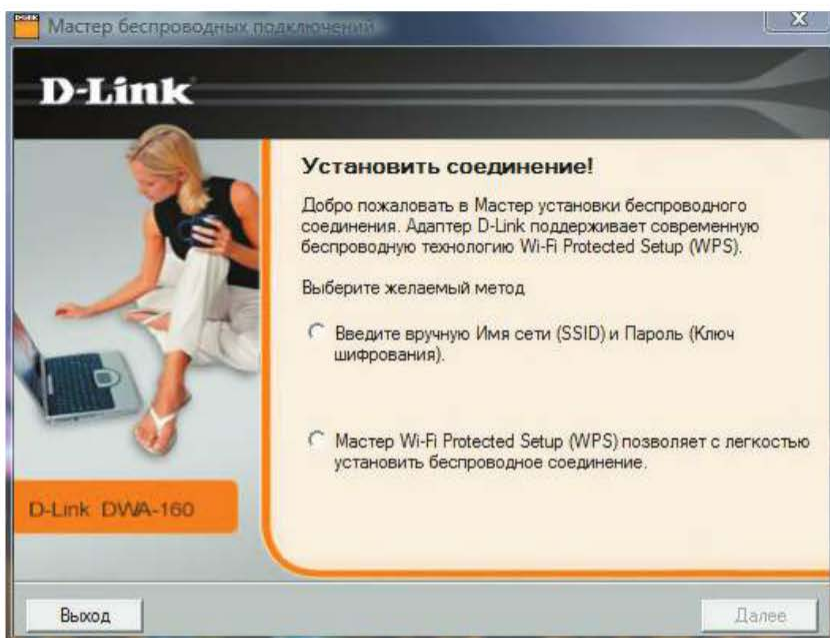


Рис. 2.6. Окно установления беспроводного соединения

2.2. Настройка точки доступа в режиме Access Point

Перед выполнением задания (рис. 2.7) верните настройки точки доступа к заводским настройкам по умолчанию. Для этого подключите точку доступа к адаптеру питания и удерживайте в течение 10 секунд кнопку *Reset*, расположенную на задней панели устройства (рис. 2.8).

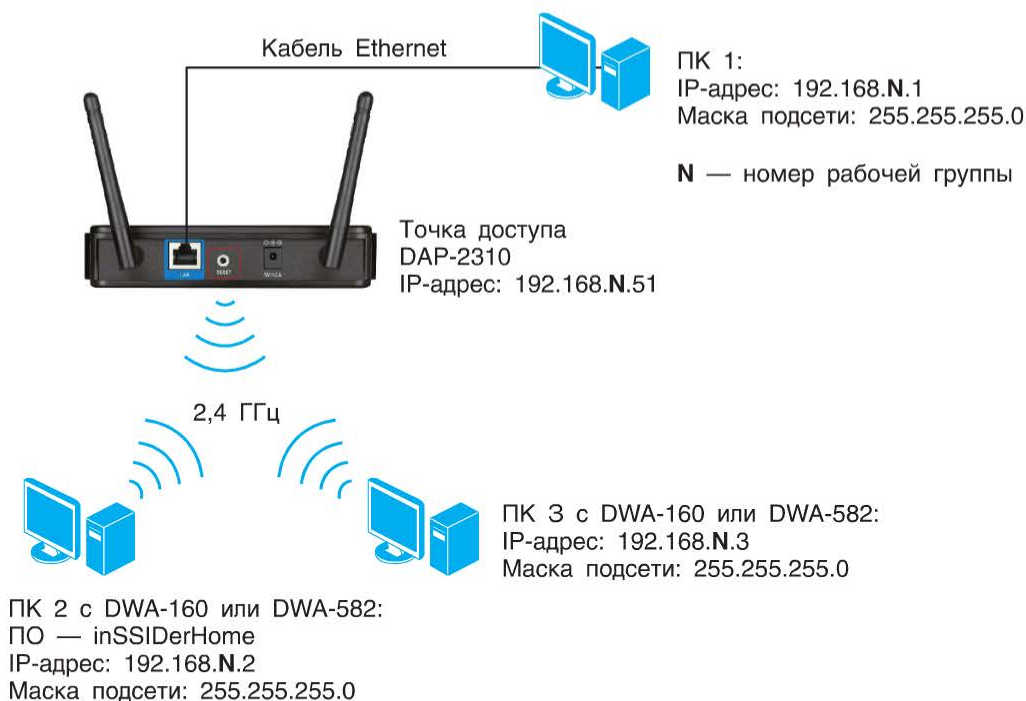


Рис. 2.7. Схема подключения рабочих станций

Шаг 1. Подключите Ethernet-кабель к LAN-порту точки доступа DAP-2310 и к сетевому адаптеру рабочей станции ПК 1.

Шаг 2. Настройте на рабочей станции ПК 1 статический IP-адрес 192.168.0.1 с маской подсети 255.255.255.0.

Шаг 3. Проверьте соединение между ПК 1 и точкой доступа с помощью команды ping:

В командной строке ПК 1 введите: ping 192.168.0.50

Примечание. IP-адрес управления точки доступа обычно указывается в руко-



Рис. 2.8. Расположение кнопки Reset на точке доступа DAP-2310

водстве пользователя. Для точки доступа D-Link DAP-2310 IP-адрес управления по умолчанию — 192.168.0.50

Шаг 4. Зайдите на Web-интерфейс точки доступа. Для этого выполните следующие действия:

1) на рабочей станции ПК 1 запустите Web-браузер, в адресной строке которого укажите IP-адрес интерфейса управления точки доступа по умолчанию: `http://192.168.0.50`;

2) в окне аутентификации (рис. 2.9) в поле *User Name* введите *admin*, поле *Password* оставьте пустым и нажмите кнопку *Login*.



Рис. 2.9. Окно аутентификации

Внимание: если на рабочей станции произведены настройки прокси-сервера, то их необходимо отключить в настройках браузеров:

Mozilla Firefox: меню *Инструменты* → *Настройки* → *Дополнительные*. Далее вкладка *Сеть* → *Настройка параметров соединения Firefox с Интернетом* → *Настроить* → *Без прокси*.

Internet Explorer: меню *Сервис* → *Свойство обозревателя*. Далее вкладка *Подключения* → *Настройка сети* → *Автоматическое определение параметров*.

После нажатия кнопки *Login* открывается окно Web-интерфейса управления точки доступа (рис. 2.10). Условно Web-интерфейс можно разделить на три области. Область 1 содержит список папок, объединяющих семейство настроек, предназначенных для выполнения той или иной задачи. В области 3 отображаются текущие настройки точки доступа и поля для их изменения (не для всех пунктов меню). В области 2 осуществляется доступ к настройкам *Administration Settings*, *Firmware and SSL Certification Upload*, *Configuration File* (пункт меню *Maintenance*), *Save and Activate*, *Discard Changes* (пункт меню *Configuration*), *System Settings* (пункт меню *System*).

Шаг 5. Уменьшите выходную мощность передатчика точки доступа до 12,5 %. Для этого выберите *Advanced Settings* → *Performance*, в списке *Transmit Power* выберите 12,5 %. Нажмите кнопку *Save* (рис. 2.11).



Рис. 2.10. Web-интерфейс управления точки доступа

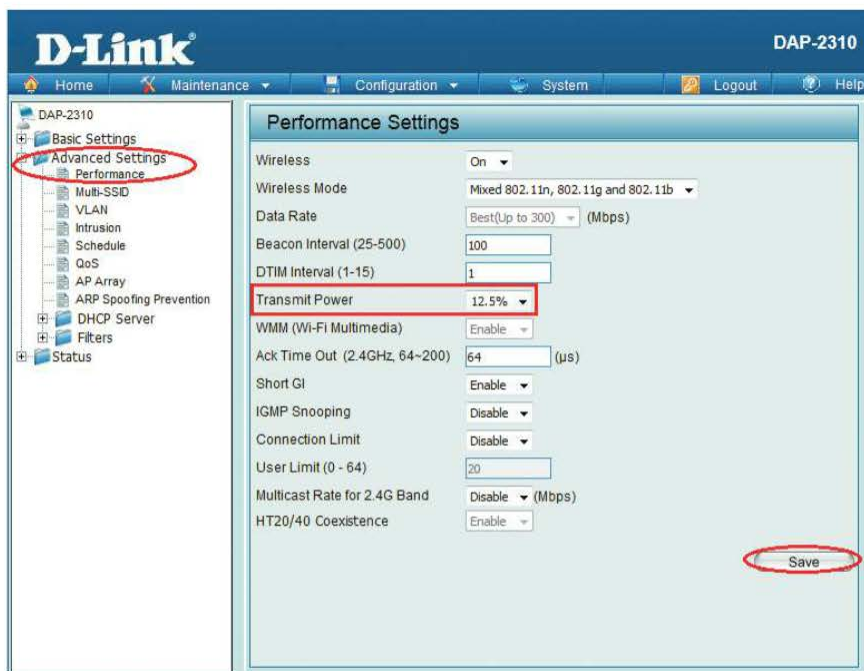


Рис. 2.11. Изменение выходной мощности передатчика

Шаг 6. Измените IP-адрес управления точки доступа. Для этого выберите раздел *Basic Settings* → *LAN*. В открывшемся окне в меню *Get IP From* выберите *Static IP (Manual)*, в поле *IP Address* введите *192.168.N.51*, в поле *Subnet Mask* введите *255.255.255.0*, поле *Default Gateway* оставьте пустым. Нажмите кнопку *Save* (рис. 2.12).



Рис. 2.12. Изменение IP-адреса управления точки доступа

Шаг 7. Сохраните и активируйте настройки. Для этого выберите *Configuration* → *Save and Activate* (рис. 2.13).



Рис. 2.13. Сохранение настроек

Шаг 8. Измените на рабочей станции ПК 1 статический IP-адрес на *192.168.N.1* с маской подсети *255.255.255.0*. В адресной строке Web-браузера введите новый IP-адрес управления точки доступа: *http://192.168.N.51*.

Шаг 9. Измените пароль администратора. Выберите *Maintenance* → *Administration Settings* (рис. 2.14). В открывшемся окне установите галочку *Login Settings*, в поле *New Password* введите *PasswordDlink* и повторите его в поле *Confirm Password*. Установите галочку *Apply New Password* и нажмите кнопку *Save* (рис. 2.15).

Шаг 10. Вернитесь на страницу аутентификации (нажмите *Logout* в правом верхнем углу Web-интерфейса). В поле *User Name* введите *admin*, в поле *Password* введите *PasswordDlink*. Нажмите кнопку *Login*.

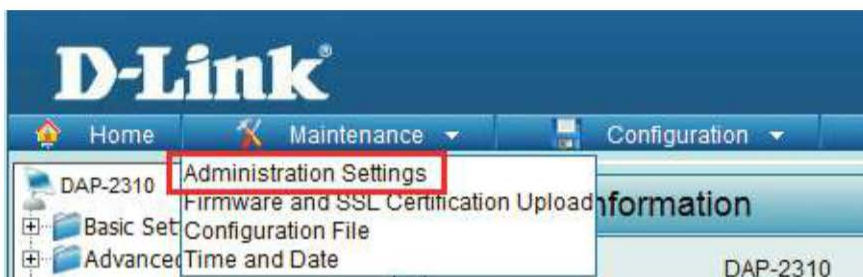


Рис. 2.14. Вход в административные настройки

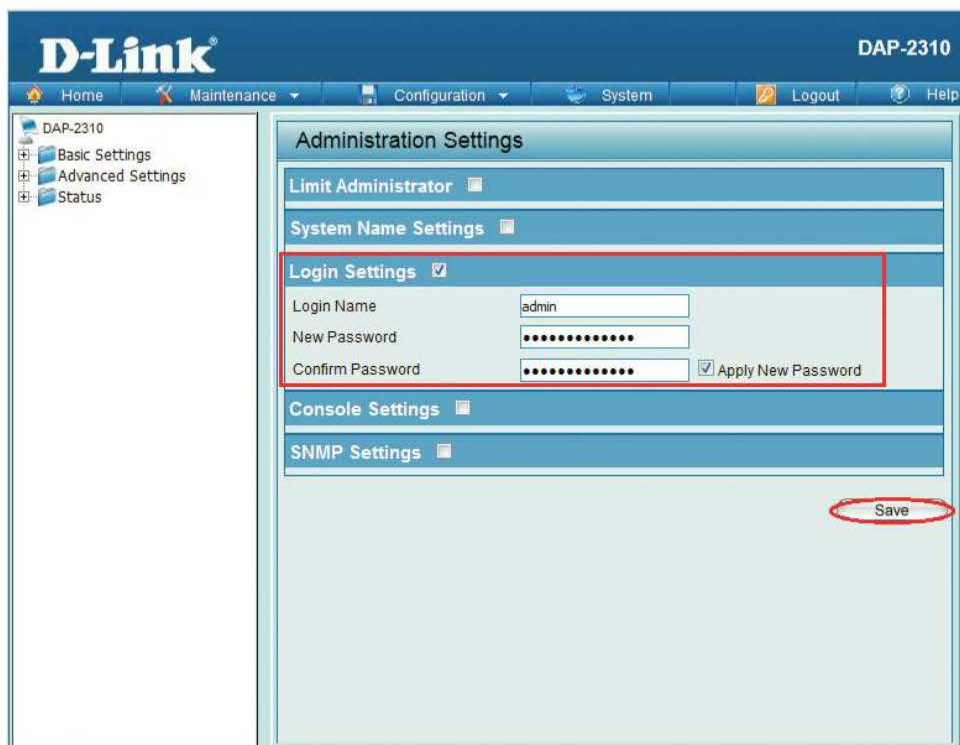


Рис. 2.15. Изменение пароля администратора

Шаг 11. Настройте режим *Access Point*, чтобы рабочие станции ПК 2 и ПК 3 могли взаимодействовать между собой через точку доступа. Для этого выполните следующие действия (рис. 2.16):

- 1) выберите раздел *Basic Settings* → *Wireless*;
- 2) в списке *Mode* выберите *Access Point*;
- 3) в поле *Network Name (SSID)* введите *class_N* (по умолчанию имя беспроводной сети *alink*);

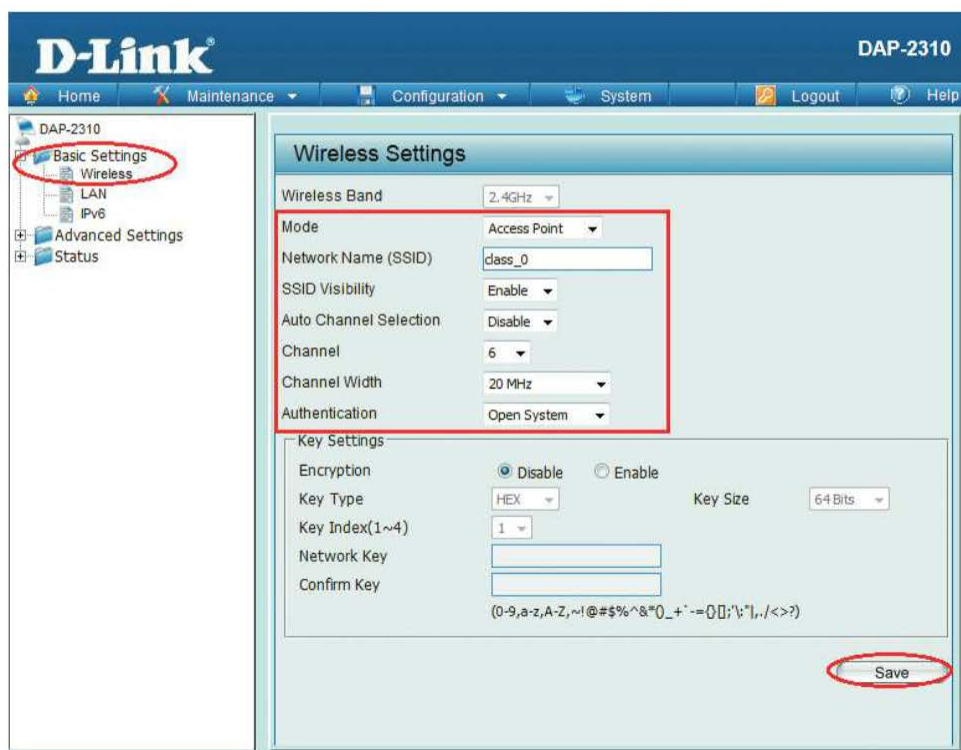


Рис. 2.16. Настройка точки доступа в режиме Access Point

- 4) отключите автоматический выбор канала. В поле *Auto Channel Selection* выберите *Disable*;
- 5) в списке *Channel* выберите 6;
- 6) в выпадающем меню *Authentication* выберите *Open System*;
- 7) для сохранения настроек нажмите кнопку *Save*.

Примечание. В данной лабораторной работе используется аутентификация открытых систем (Open System). Настройка других методов аутентификации рассматривается в лабораторной работе № 6.

Шаг 12. Сохраните и активируйте настройки. Выберите *Configuration* → *Save and Activate*.

Шаг 13. Настройте статические IP-адреса на беспроводных интерфейсах ПК 2 и ПК 3 в соответствии с рис. 2.7 и номером рабочей группы.

Шаг 14. Подключитесь на рабочих станциях ПК 2 и ПК 3 к беспроводной сети *class_N*. Из списка доступных беспроводных сетей выберите сеть с идентификатором SSID *class_N*, снимите галочку *Подключаться автоматически* и нажмите кнопку *Подключение*.

Шаг 15. Проверьте соединение между ПК 2 и ПК 3 с помощью команды ping:

в командной строке ПК 2 введите: ping 192.168.N.3
ответил ПК 3? _____

в командной строке ПК 3 введите: ping 192.168.N.2
ответил ПК 2? _____

Шаг 16. Просмотрите информацию о клиентах, подключенных через точку доступа. С рабочей станции ПК 1 зайдите на Web-интерфейс точки доступа, выберите *Status* → *Client Information* (рис. 2.17).



Client Information Station association (2.4GHz) : 2						
SSID	MAC	Band	Authentication	RSSI	Power Saving Mode	
Primary SSID	C0:A0:BB:57:68:B8	N	OPEN	94%	Off	
Primary SSID	98:0D:2E:70:A9:70	G	OPEN	97%	On	

Рис. 2.17. Информация о клиентах, подключенных к беспроводной сети *class_N*

Шаг 17. Отключитесь на рабочих станциях ПК 2 и ПК 3 от беспроводной сети *class_N*.

Шаг 18. Настройте на точке доступа динамическое распределение IP-адресов. Для этого выберите *Advanced Settings* → *DHCP Server* → *Dynamic Pool*



D-Link DAP-2310

Navigation: Home | Maintenance | Configuration | System | Logout | Help

Left sidebar: Basic Settings, Advanced Settings (Performance, Multi-SSID, VLAN, Intrusion, Schedule, QoS, AP Array, ARP Spoofing Prevention, DHCP Server, Dynamic Pool Settings, Static Pool Settings, Current IP Mapping List), Filters, Status

Dynamic Pool Settings

DHCP Server Control
Function Enable/Disable: Enable

Dynamic Pool Settings

IP Assigned From	192.168.0.20
The Range of Pool (1-254)	20
Subnet Mask	255.255.255.0
Gateway	
WINS	
DNS	
Domain Name	dlink-ap
Lease Time (60 - 31536000 sec)	604800

Save

Рис. 2.18. Настройка DHCP-сервера на точке доступа

Проверьте загруженность канала, на который настроена точка доступа DAP-2310. Чтобы в окне inSSIDer отображалась информация о беспроводных сетях, работающих на 6 канале, в области *FILTERS* в поле *Channel* введите 6. Нажмите клавишу *Enter* (рис. 2.20).

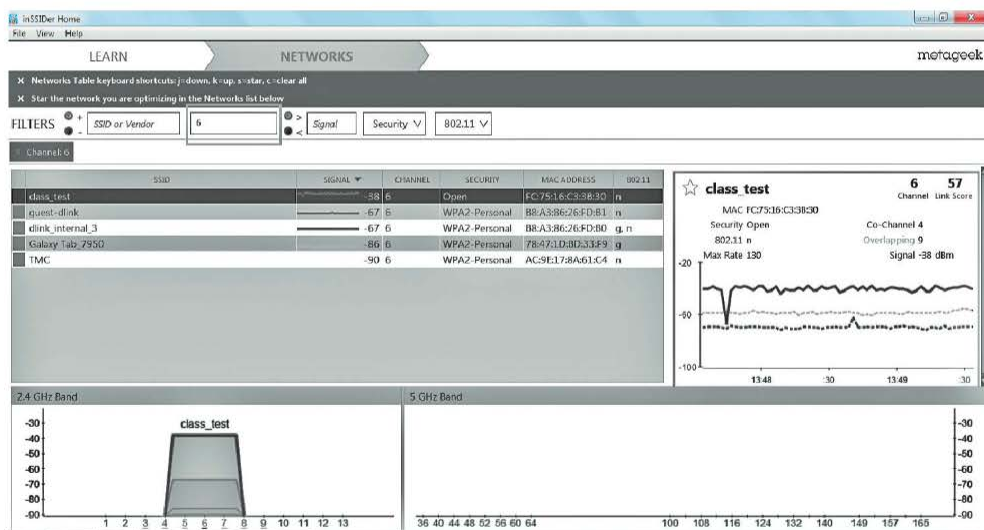


Рис. 2.20. Определение загруженности 6-го канала

Сколько беспроводных сетей работает на 6-м канале? _____

Проверьте загруженность всех каналов.

Какой канал наименее загружен? _____

Примечание. Выбор оптимального по загруженности канала позволит уменьшить межканальную интерференцию.

Шаг 2. Настройте точку доступа на работу в наименее загруженном канале. Для этого с рабочей станции ПК 1 зайдите на Web-интерфейс точки доступа, выберите раздел *Basic Settings* → *Wireless*. В списке *Channel* выберите наиболее свободный канал и нажмите *Save*. Сохраните и активируйте настройки *Configuration* → *Save and Activate*.

Шаг 3. В программе inSSIDer можно отследить изменение уровня сигнала беспроводной сети в режиме реального времени. Проанализируйте уровни сигналов с помощью inSSIDer.

Определите уровень сигнала беспроводной сети *class_N*? _____

Определите уровни сигналов беспроводных сетей других рабочих групп? _____

Шаг 4. Отключитесь на рабочих станциях ПК 2 и ПК 3 от беспроводной сети *class_N*.

Шаг 5. Настройте на беспроводных интерфейсах ПК 2 и ПК 3 статические IP-адреса в соответствии с рис. 2.7 и номером рабочей группы.

2.4. Настройка точки доступа в режиме Wireless Client

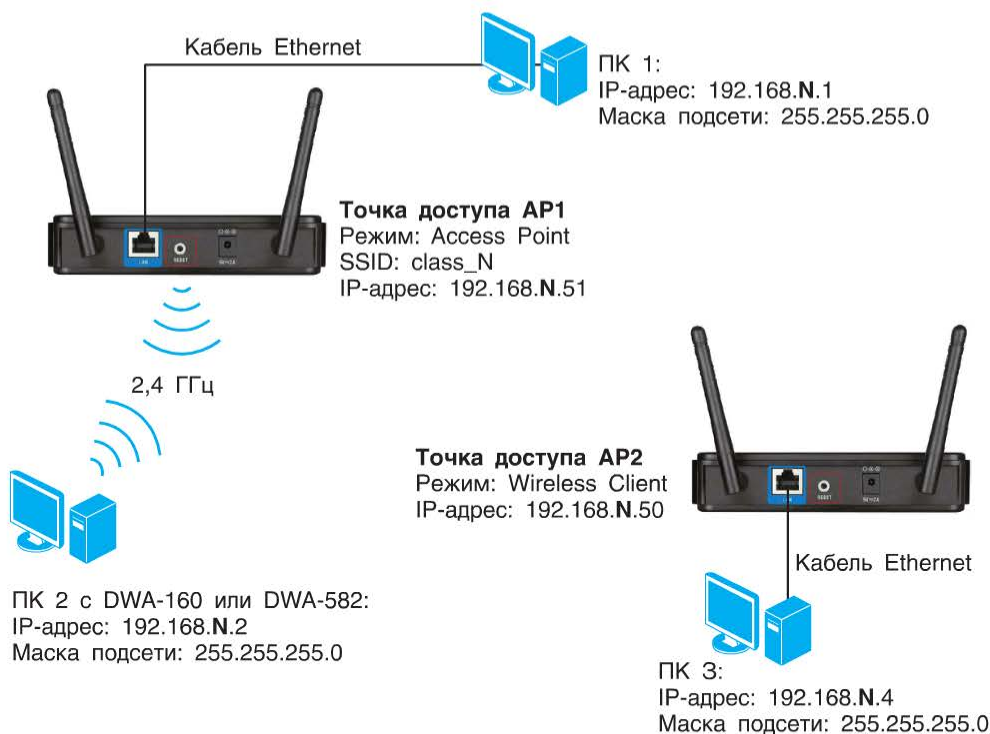


Рис. 2.21. Схема сети для п. 2.4

Примечание. Настройки точки доступа AP1, выполненные в п. 2.2, остаются без изменений. Режим Wireless Client настраивается только на точке доступа AP2.

Шаг 1. Верните настройки точки доступа AP2 к заводским настройкам по умолчанию. Для этого нажмите и удерживайте кнопку *Reset* в течение 10 секунд.

Шаг 2. Отключите беспроводной адаптер ПК 3 в настройках Windows. Соедините рабочую станцию ПК 3 и точку доступа AP2 Ethernet-кабелем.

Шаг 3. Настройте на Ethernet адаптере рабочей станции ПК 3 статический IP-адрес 192.168.0.4 с маской подсети 255.255.255.0.

Шаг 4. Зайдите на Web-интерфейс точки доступа AP2 и измените IP-адрес управления по умолчанию на 192.168.N.50 с маской подсети 255.255.255.0. Сохраните и активируйте настройки.

Шаг 5. Измените IP-адрес на Ethernet-адаптере ПК 3 на 192.168.N.4 с маской подсети 255.255.255.0.

Шаг 6. Повторно зайдите на Web-интерфейс точки доступа AP2 и уменьшите выходную мощность передатчика точки доступа до 12,5 %. Выберите *Advanced Settings* → *Performance*, в списке *Transmit Power* выберите 12,5 %. Нажмите кнопку *Save*.

Шаг 7. Настройте на точке доступа AP2 режим работы *Wireless Client*. Для этого выберите раздел *Basic Settings* → *Wireless*, в выпадающем списке *Mode* выберите *Wireless Client*. В области *Site Survey* нажмите *Scan* для поиска доступных беспроводных сетей. Выберите беспроводную сеть *class_N* и нажмите кнопку *Save*. Сохраните и активируйте настройки: *Configuration* → *Save and Activate* (рис. 2.22).

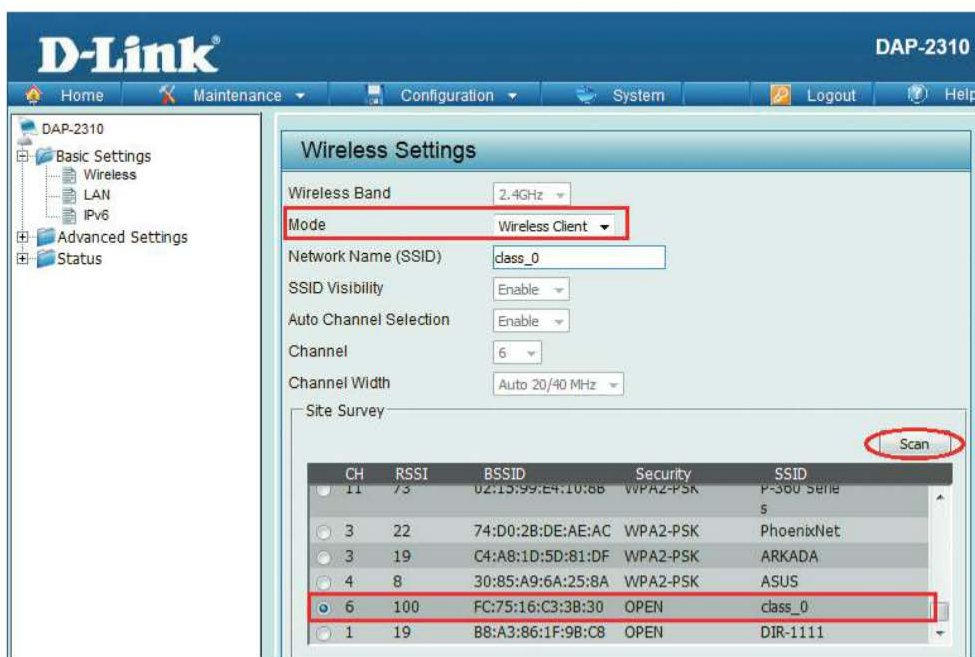


Рис. 2.22. Настройка точки доступа в режиме Wireless Client

Шаг 8. На рабочей станции ПК 2 подключитесь к беспроводной сети *class_N*.

Шаг 9. Проверьте соединение между ПК 2 и ПК 3 с помощью команды ping: в командной строке ПК 2 введите: ping 192.168.N.4

ответил ПК 3? _____

в командной строке ПК 3 введите: ping 192.168.N.2

ответил ПК 2? _____

Шаг 10. Верните настройки точки доступа AP2 к заводским настройкам по умолчанию. Для этого выберите *System* → *Restore to Factory Default Settings* (рис. 2.23).



Рис. 2.23. Сброс настроек к заводским настройкам по умолчанию

Шаг 11. Отключите рабочую станцию ПК 3 от точки доступа AP2.

2.5. Настройка точки доступа в режиме AP Repeater

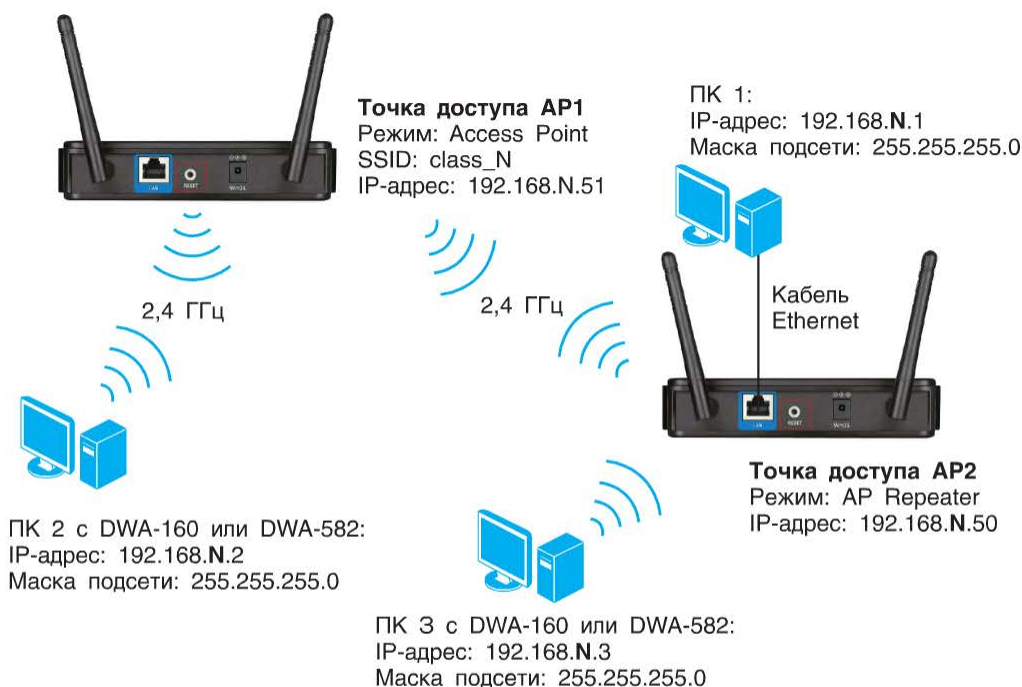


Рис. 2.24. Схема сети для п. 2.5

Примечание. Настройки точки доступа AP1, выполненные в п. 2.2, остаются без изменений. Режим AP Repeater настраивается только на точке доступа AP2.

Шаг 1. Включите беспроводной адаптер ПК 3 в настройках Windows и настройте на беспроводном интерфейсе статический IP-адрес 192.168.N.3 с маской подсети 255.255.255.0.

Шаг 2. Подключите рабочую станцию ПК 1 к LAN-порту точки доступа AP2. Измените статический IP-адрес сетевого адаптера на 192.168.0.1 с маской подсети 255.255.255.0.

Шаг 3. С ПК 1 зайдите на Web-интерфейс точки доступа AP2 и измените IP-адрес управления по умолчанию на 192.168.N.50 с маской подсети 255.255.255.0. Сохраните и активируйте настройки.

Шаг 4. Измените IP-адрес ПК 1 на 192.168.N.1 с маской подсети 255.255.255.0.

Шаг 5. Повторно зайдите на Web-интерфейс точки доступа AP2 и уменьшите выходную мощность передатчика точки доступа до 12,5 %.

Шаг 6. Настройте на точке доступа AP2 режим работы *AP Repeater*. Для этого выберите раздел *Basic Settings* → *Wireless*, в выпадающем списке *Mode* выберите *AP Repeater*. В области *Site Survey* нажмите *Scan* для поиска доступных беспроводных сетей. Выберите беспроводную сеть *class_N* и нажмите

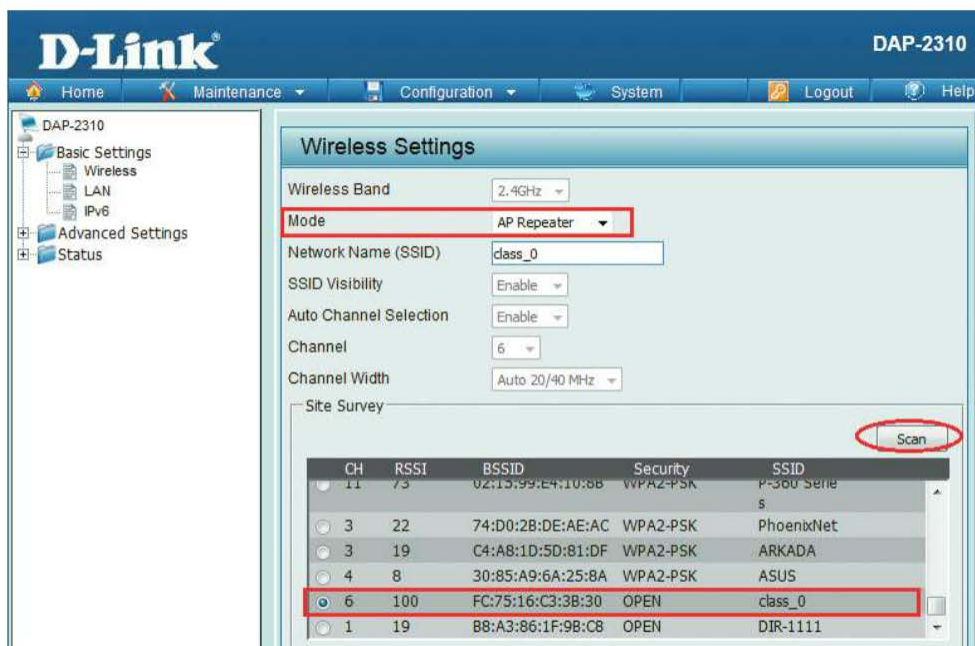


Рис. 2.25. Настройка точки доступа в режиме AP Repeater

кнопку *Save*. Сохраните и активируйте настройки *Configuration* → *Save and Activate* (рис. 2.25).

Шаг 7. На ПК 2 и ПК 3 подключитесь к беспроводной сети *class_N*.

Шаг 8. Проверьте соединение между ПК 2 и ПК 3 с помощью команды *ping*:

в командной строке ПК 2 введите: `ping 192.168.N.3`
ответил ПК 3? _____

в командной строке ПК 3 введите: `ping 192.168.N.2`
ответил ПК 2? _____

Шаг 9. Просмотрите информацию о клиентах, ассоциированных с точкой доступа. На точках доступа AP1 и AP2 выберите *Status* → *Client Information*.

К какой точке доступа подключены клиенты ПК 2 и ПК 3? _____

Лабораторная работа № 3. Объединение инфраструктурных BSS с единым SSID через распределительную систему

Распределительная система и инфраструктурные BSS позволяют создавать беспроводные сети любой протяженности и сложности. В стандарте IEEE

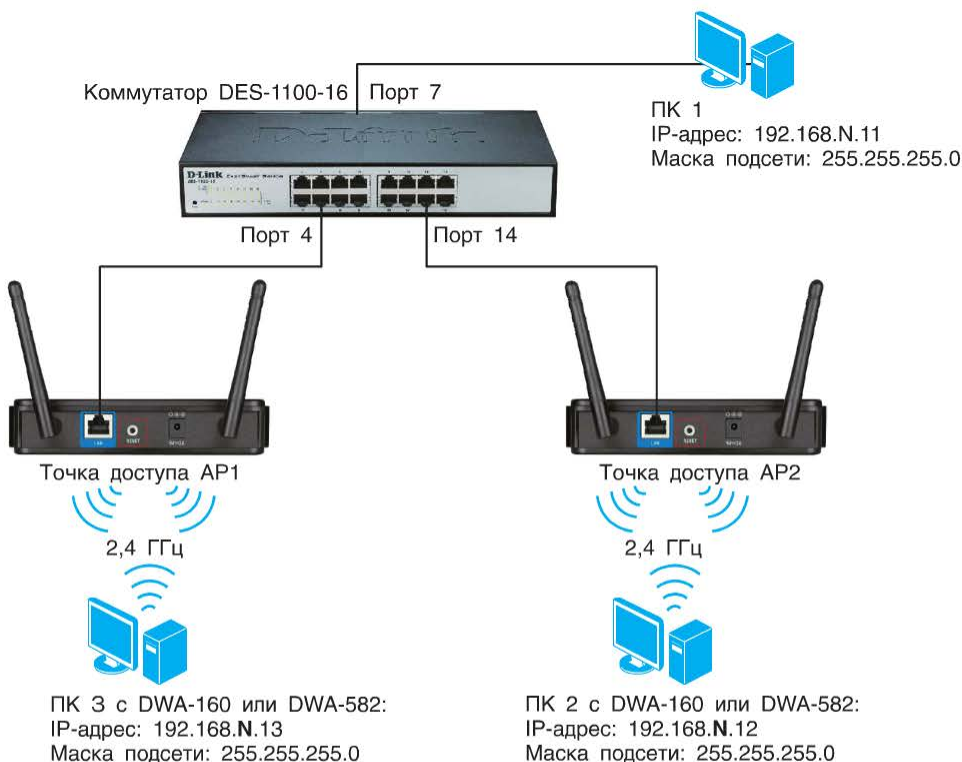


Рис. 3.1. Общая схема сети

802.11 такие сети называются расширенным набором услуг (*Extended Service Set*, ESS). ESS состоит из двух и более инфраструктурных BSS с единым SSID, соединенных распределительной системой. Сама распределительная система при этом не входит в ESS. Все станции внутри ESS могут взаимодействовать друг с другом, а мобильные станции могут переходить из одного BSS в другой в пределах ESS, не теряя связи с сетью. Для интеграции архитектуры IEEE 802.11 с проводной сетью используется портал. Логика портала реализуется в устройстве (коммутаторе или маршрутизаторе), являющемся частью проводной локальной сети и присоединенном к распределительной системе.

Оборудование (на 2 рабочих места):

Рабочая станция	3 шт.
Беспроводной адаптер DWA-160 или DWA-582	2 шт.
Точка доступа DAP-2310	2 шт.
Коммутатор DES-1100-16	1 шт.
Кабель Ethernet	3 шт.

Цель работы: изучить объединение инфраструктурных BSS с одним именем SSID через распределительную систему.

Перед выполнением задания (рис. 3.1) верните настройки точек доступа и коммутатора к заводским настройкам по умолчанию.

П р и м е ч а н и е . Настройка точек доступа выполняется с рабочей станции ПК 1.

3.1. Изменение IP-адреса управления точек доступа AP1 и AP2

Шаг 1. Подключите Ethernet-кабель к LAN-порту точки доступа AP1 и к сетевому адаптеру рабочей станции ПК 1.

Шаг 2. Настройте статический IP-адрес на Ethernet-адаптере рабочей станции ПК 1 — 192.168.0.11 с маской подсети 255.255.255.0.

Шаг 3. Зайдите на Web-интерфейс точки доступа AP1. Измените IP-адрес управления на 192.168.N.50 с маской подсети 255.255.255.0. Сохраните и активируйте настройки.

Шаг 4. Подключите рабочую станцию ПК 1 к LAN-порту точки доступа AP2.

Шаг 5. Зайдите на Web-интерфейс точки доступа AP2. Измените IP-адрес управления на 192.168.N.51 с маской подсети 255.255.255.0. Сохраните и активируйте настройки.

Шаг 6. Измените IP-адрес Ethernet-адаптера рабочей станции ПК 1 на 192.168.N.11 с маской подсети 255.255.255.0.

3.2. Настройка точки доступа AP1

Шаг 1. Подключите ПК 1 к LAN-порту точки доступа AP1. Зайдите на Web-интерфейс и уменьшите выходную мощность передатчика точки доступа до 12,5 %.

Шаг 2. Создайте беспроводную сеть в режиме *Access Point* с SSID *Dlink_N*:

- 1) выберите раздел *Basic Settings* → *Wireless*;
- 2) в списке *Mode* выберите *Access Point*;
- 3) в поле *Network Name (SSID)* введите *Dlink_N*;
- 4) отключите автоматический выбор канала. Для этого в поле *Auto Channel Selection* выберите *Disable*;
- 5) в поле *Channel* выберите 6;

Примечание. Точки доступа настраиваются на неперекрывающиеся каналы для уменьшения влияния интерференции.

- 6) в выпадающем меню *Authentication* выберите *Open System*;
- 7) сохраните настройку, нажав кнопку *Save*.

Шаг 3. Сохраните и активируйте настройки. Выберите *Configuration* → → *Save and Activate*.

3.3. Настройка точки доступа AP2

Шаг 1. Подключите ПК 1 к LAN-порту точки доступа AP2. Зайдите на Web-интерфейс и уменьшите выходную мощность передатчика точки доступа до 12,5 %.

Шаг 2. Создайте беспроводную сеть в режиме *Access Point* с SSID *Dlink_N*. Для этого:

- 1) выберите раздел *Basic Settings* → *Wireless*;
- 2) в списке *Mode* выберите *Access Point*;
- 3) в поле *Network Name (SSID)* введите *Dlink_N*;
- 4) отключите автоматический выбор канала. Для этого в поле *Auto Channel Selection* выберите *Disable*;
- 5) в поле *Channel* выберите 11;
- 6) в выпадающем меню *Authentication* выберите *Open System*;
- 7) сохраните настройки, нажав кнопку *Save*.

Шаг 3. Сохраните и активируйте настройки. Выберите *Configuration* → → *Save and Activate*.

3.4. Проверка работоспособности схемы

Шаг 1. Подключите устройства, как показано на рис. 3.1.

Шаг 2. Настройте статические IP-адреса на беспроводных интерфейсах ПК 2 и ПК 3 в соответствии с рис. 3.1 и номером рабочей группы.

Шаг 3. Подключитесь на рабочих станциях ПК 2 и ПК 3 к беспроводной сети *Dlink_N*.

Шаг 4. Проверьте соединение между рабочими станциями командой ping:
 от ПК 1 к ПК 2 и ПК 3 _____
 от ПК 2 к ПК 1 и ПК 3 _____
 от ПК 3 к ПК 1 и ПК 2 _____

Шаг 5. Просмотрите, к какой точке доступа подключены беспроводные клиенты. На точках доступа AP1 и AP2 выберите *Status* → *Client Information* (рис. 3.2).

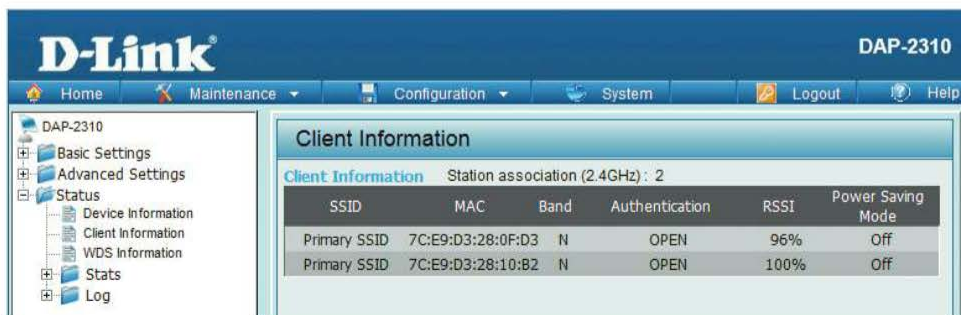


Рис. 3.2. Информация о клиентах, подключенных к беспроводной сети *Dlink_N*

К какой точке доступа подключены беспроводные клиенты? _____

Шаг 6. Просмотрите MAC-адреса на беспроводных интерфейсах ПК 2 и ПК 3. Для этого в командной строке введите: `getmac`

MAC-адрес ПК 2 _____
 MAC-адрес ПК 3 _____

Шаг 7. Отключите питание одной точки доступа, с которой ассоциированы беспроводные клиенты. Клиенты переподключились к другой точке доступа? _____

Шаг 8. Проверьте соединение между рабочими станциями командой ping:
 от ПК 1 к ПК 2 и ПК 3 _____
 от ПК 2 к ПК 1 и ПК 3 _____
 от ПК 3 к ПК 1 и ПК 2 _____

Шаг 9. Подключите ранее отключенное питание к точке доступа.

Шаг 10. Включите функцию *Link Integrity* на точках доступа AP1 и AP2. Для этого выберите *Advanced Settings* → *Filters* → *WLAN Partition*. В списке *Link Integrity* выберите *Enable* и нажмите кнопку *Save* (рис. 3.3). Сохраните

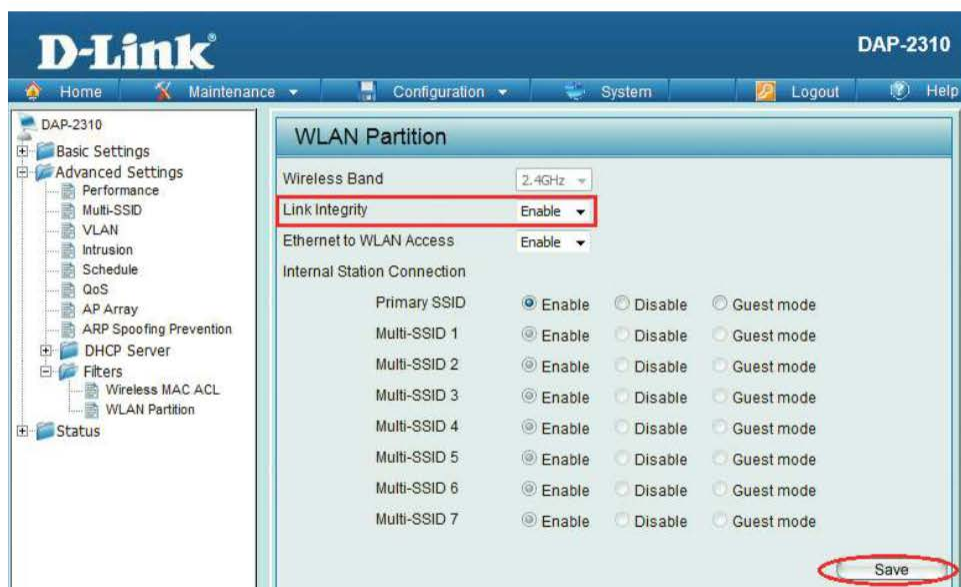


Рис. 3.3. Включение функции *Link Integrity*

и активируйте настройки. Для этого выберите *Configuration* → *Save and Activate*. Дождитесь перезагрузки точки доступа.

Примечание. Если Ethernet-канал между LAN и точкой доступа отключается, то включенная функция *Link Integrity* позволяет автоматически разрывать ассоциацию беспроводных клиентов с точкой доступа.

Шаг 11. Отключите точки доступа AP1 и AP2 от коммутатора.

Произошел разрыв ассоциации беспроводных клиентов? _____

Шаг 12. Подключите точки доступа к портам коммутатора. Подключитесь к беспроводной сети *Dlink_N*. Отключите функцию *Link Integrity* на точках доступа AP1 и AP2.

Лабораторная работа № 4. Исследование кадров MAC стандарта IEEE 802.11

В стандарте IEEE 802.11 определены три типа кадров:

- кадры данных или информационные кадры (*data frames*) — используются для передачи данных;
- контрольные кадры (*control frames*) — служат для контроля доступа к среде;
- кадры управления (*management frames*) — используются для обмена управляющей информацией при выполнении таких операций подуровня MAC, как ассоциация и разрыв ассоциации станции с точкой доступа, аутентификация и отмена аутентификации, синхронизация и др.

Каждый кадр MAC состоит из следующих основных компонентов (рис. 4.1): заголовка кадра, тела кадра переменной длины и контрольной суммы кадра. Первые три поля («Управление кадром», «Длительность/идентификатор», «Адрес 1») и последнее поле («Контрольная сумма кадра») присутствуют во всех кадрах MAC. Остальные поля («Адрес 2», «Адрес 3», «Управление очередностью», «Адрес 4», «Управление QoS», «Тело кадра») присутствуют только в определенных кадрах MAC.

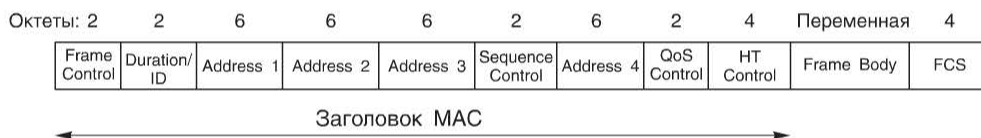


Рис. 4.1. Формат кадра MAC IEEE 802.11-2012

Каждый тип кадра имеет несколько подтипов в зависимости от выполняемой операции.

Ниже описаны поля общего формата кадра.

- Управление кадром (*Frame Control*): поле состоит из 11 подполей и служит для указания типа и подтипа кадра, а также предоставления управляющей информации (формат поля описан ниже).

- Длительность/идентификатор (*Duration/ID*): значение этого поля зависит от типа и подтипа кадра. Например, в кадрах данных и некоторых контрольных кадрах это поле содержит значение длительности соединения, которое используется для установки вектора сетевого распределения NAV (*Network Allocation Vector*). В контрольных кадрах PS-Poll это поле содержит идентификатор станции (AID, Association ID).

- Адреса 1–4 (*Address 1–4*): четыре поля адреса используются для указания идентификатора BSSID, адреса источника (SA), адреса назначения (DA), адреса передающей станции (TA) и адреса принимающей станции (RA). Количество и значения полей адреса зависят от типа кадра.

- Управление очередностью (*Sequence Control*): поле используется при фрагментации и служит для определения порядка фрагментов, принадлежащих одному кадру, и предотвращения их дублирования. Оно состоит из двух подполей: «Номер фрагмента» (*Fragment Number* длиной 4 бит), указывающего номер фрагмента кадра, и «Порядковый номер» (*Sequence Number* длиной 12 бит), содержащего порядковый номер кадра.

- Управление QoS (*QoS Control*): поле было добавлено в заголовок MAC после появления дополнения к стандарту IEEE 802.11e.

- Управление высокой пропускной способностью (*HT Control*): поле было добавлено в заголовок кадра MAC после появления спецификации 802.11n. После принятия спецификации 802.11ac это поле стало иметь два варианта: HT и VHT. Оно всегда присутствует в кадрах упаковщика контрольных кадров (*Control Wrapper*), а также в кадрах данных и кадрах управления с сервисом QoS, на что указывает бит «Порядок» поля «Управление кадром».

• Тело кадра (*Frame Body*): поле переменной длины, содержащее информацию, специфичную для каждого типа кадра. Минимальный размер этого поля — 0 байт, максимальный размер определяется максимальными размерами блока данных сервиса MAC (MSDU), агрегированного MSDU (A-MSDU) и блока данных протокола MAC (MPDU), поддерживаемыми получателями; максимальной длительностью блока данных физического уровня; полями, присутствующими в заголовке MAC (QoS Control, HT Control); наличием шифрования.

• Контрольная сумма кадра (*FCS*): поле длиной 32 бит, предназначенное для проверки четности с избыточностью. Вычисляется на основе всех полей заголовка и поля «Тело кадра».

Поле «Управление кадром» длиной 16 бит состоит из 11 подполей (рис. 4.2):

B0	B1	B2	B3	B4	B7	B8	B9	B10	B11	B12	B13	B14	B15
Protocol Version	Type	Subtype	To DS	From DS	More Fragments	Retry	Power Management	More Data	Protected Frame	Order			
Биты:	2	2	4	1	1	1	1	1	1	1	1	1	1

Рис. 4.2. Поле «Управление кадром»

• Версия протокола (*Protocol Version*): определяет версию протокола 802.11. Используемая в настоящее время версия протокола — 0. Остальные значения зарезервированы для будущего использования.

• Тип и подтип (*Type, Subtype*): эти поля совместно определяют назначение кадра: контроль, управление или данные. Каждый тип кадра имеет несколько подтипов.

• Направление кадра к DS (*To DS*): значение этого поля равно 1, если кадр предназначен распределительной системе или станция передает кадр другой станции через точку доступа той же BSS. Во всех остальных кадрах значение поля равно 0.

• Направление кадра от DS (*From DS*): значение этого поля равно 1, если кадр исходит из распределительной системы или точки доступа. Во всех остальных кадрах значение поля равно 0.

• Больше фрагментов (*More Fragments*): значение этого поля равно 1 во всех кадрах данных и кадрах управления, если за данным фрагментом следует несколько фрагментов, принадлежащих одному кадру. Во всех остальных кадрах значение поля равно 0.

• Повтор (*Retry*): значение поля равно 1 в любом кадре данных или кадре управления, если он является повторной передачей предыдущего. Во всех остальных кадрах значение поля равно 0. Станция-получатель использует эту информацию для исключения дублирования кадров.

• Управление мощностью (*Power management*): поле используется для указания режима управления питанием станции после успешного завершения цикла обмена кадрами. Значение поля, равное 1, указывает, что станция на-

ходится в режиме энергосбережения (*PS mode*). Значение 0 показывает, что станция находится в активном режиме.

- Больше данных (*More Data*): поле используется в кадрах данных или кадрах управления, передаваемых точкой доступа станции, находящейся в режиме энергосбережения. Значение поля, равное 1, говорит, что на точке доступа буферизировано более одного блока данных, предназначенных для этой станции.

- Защищенный кадр (*Protected Frame*): значение этого поля равно 1, если поле «Тело кадра» содержит информацию, обработанную с помощью криптографического алгоритма.

- Порядок (*Order*): значение поля равно 1:

а) в кадрах данных без поддержки QoS, которые должны обрабатываться с использованием строгоупорядоченного класса сервиса (*Strictly Ordered service class*), т. е. строго по порядку;

б) в кадрах данных или кадрах управления с сервисом QoS для указания, что кадр содержит поле «Управление высокой пропускной способностью» (*HT Control*).

За исключением этих двух случаев значение поля равно 0.

В лабораторной работе для анализа беспроводного трафика используется сетевой анализатор Microsoft Network Monitor 3.4, предназначенный для захвата и анализа пакетов в сетях Ethernet и беспроводных сетях стандарта IEEE 802.11 a/b/g/n/ac.

Используя данную программу, можно не только осуществлять мониторинг и анализ трафика в режиме реального времени, но и сохранять захваченные пакеты в файл для их последующего исследования. Сетевой анализатор Microsoft Network Monitor имеет графический интерфейс, обладает широкими возможностями фильтрации информации по многим критериям, отображает структуру кадра с высокой детализацией.

Оборудование (на 1 рабочее место):

Рабочая станция	2 шт.
Беспроводной адаптер DWA-160 или DWA-582	2 шт.
Точка доступа DAP-2310	1 шт.
Кабель Ethernet	1 шт.
ПО — анализатор трафика Microsoft Network Monitor 3.4.	

Цель работы: исследование кадров MAC стандарта IEEE 802.11.

4.1. Захват трафика с помощью сетевого анализатора Microsoft Network Monitor

Перед выполнением задания (рис. 4.3) верните настройки точки доступа к заводским настройкам по умолчанию.

Примечание. Настройка точки доступа выполняется с рабочей станции ПК 1.



Рис. 4.3. Схема сети для п. 4.1

Шаг 1. Подключите Ethernet-кабель к LAN-порту точки доступа и к Ethernet-адаптеру рабочей станции ПК 1.

Шаг 2. Настройте статический IP-адрес на Ethernet-адаптере рабочей станции ПК 1 — 192.168.0.1 с маской подсети 255.255.255.0.

Шаг 3. Зайдите на Web-интерфейс точки доступа. Измените IP-адрес управления на 192.168.N.50 с маской подсети 255.255.255.0. Сохраните и активируйте настройки.

Шаг 4. Измените IP-адрес Ethernet-адаптера рабочей станции ПК 1 на 192.168.N.1 с маской подсети 255.255.255.0.

Шаг 5. Уменьшите выходную мощность передатчика точки доступа до 12,5 %.

Шаг 6. Создайте беспроводную сеть с SSID *class_N*. Для этого:

- 1) выберите раздел *Basic Settings* → *Wireless*;
- 2) в списке *Mode* выберите *Access Point*;
- 3) в поле *Network Name (SSID)* введите *class_N*;
- 4) отключите автоматический выбор канала. Для этого в поле *Auto Channel Selection* выберите *Disable*;

- 5) в поле *Channel* выберите 6;
- 6) в выпадающем меню *Authentication* выберите *Open System*;
- 7) сохраните настройки, нажав кнопку *Save*.

Шаг 7. Сохраните и активируйте настройки. Для этого выберите *Configuration* → *Save and Activate*.

Шаг 8. Отключите Ethernet-кабель от точки доступа.

Шаг 9. Настройте статические IP-адреса на беспроводных интерфейсах ПК 1 и ПК 2 в соответствии с рис. 4.3 и номером рабочей группы.

Шаг 10. Запустите на рабочей станции ПК 1 сетевой анализатор Microsoft Network Monitor. Интерфейс программы показан на рис. 4.4.

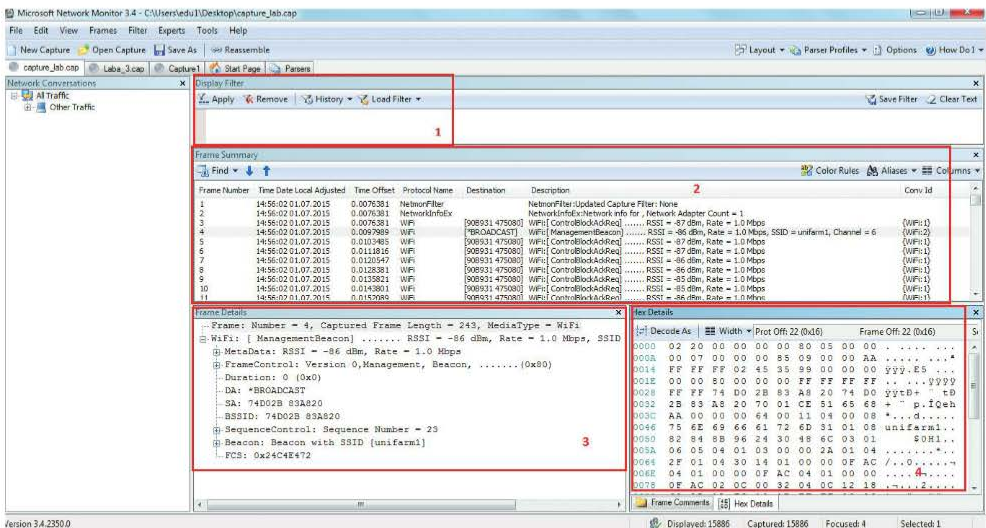


Рис. 4.4. Интерфейс Microsoft Network Monitor

Интерфейс Microsoft Network Monitor состоит из нескольких окон. В окне 1 можно создавать фильтры, позволяющие выбирать определенные кадры для их анализа. В окне 2 содержится список всех захваченных кадров, организованный в виде таблицы с заголовками. Выделяя строку таблицы, более подробную информацию о кадре и его расшифровку можно посмотреть в окне 3. Окно 4 содержит код кадра в шестнадцатеричном и текстовом представлении.

Шаг 11. Выберите интерфейс, с которого будет выполняться захват трафика, и активируйте функцию мониторинга на беспроводном адаптере. Для этого нажмите *New Capture* → *Capture Settings* (рис. 4.5).

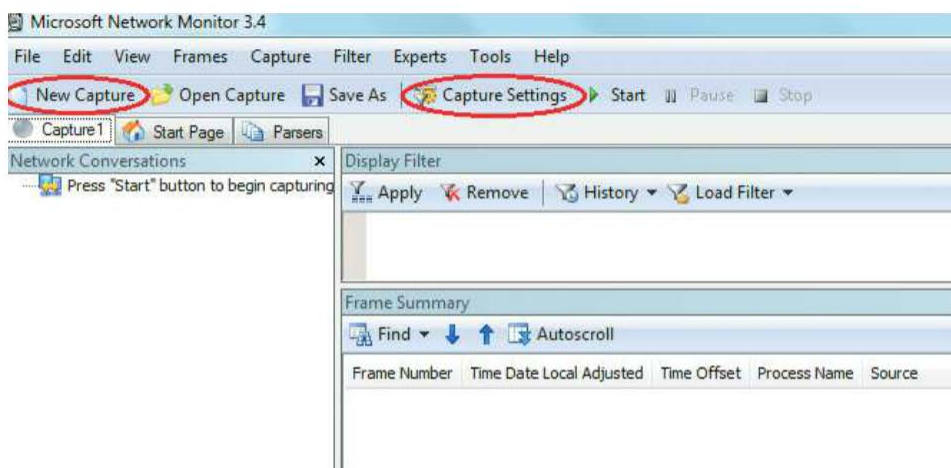


Рис. 4.5. Настройка беспроводного адаптера для захвата трафика

В открывшемся окне установите галочку *Беспроводное сетевое соединение* и нажмите *Properties* (рис. 4.6). В окне *Network Interface Configuration* нажмите кнопку *Scanning Options* (рис. 4.7).

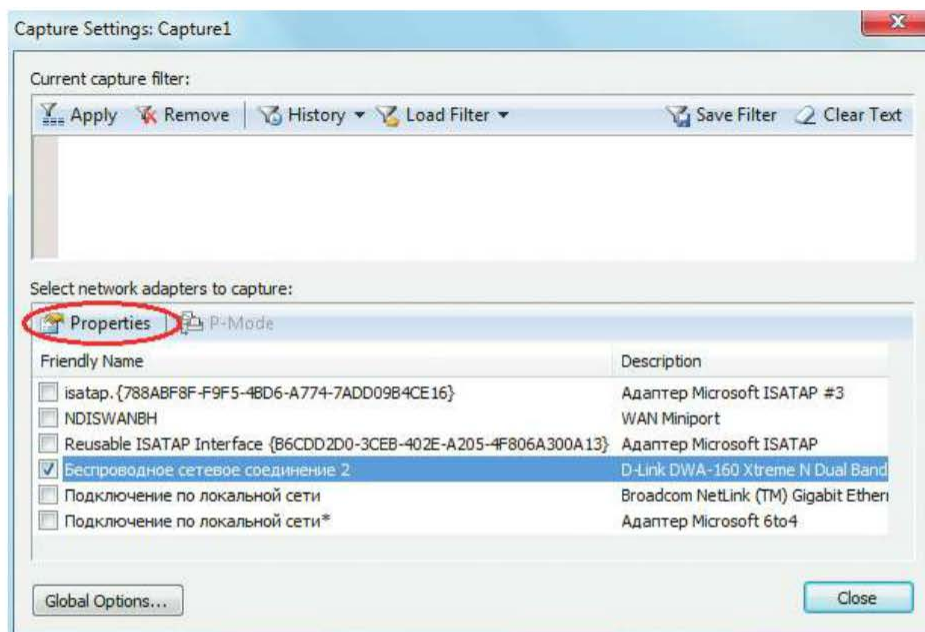


Рис. 4.6. Выбор интерфейса для захвата трафика

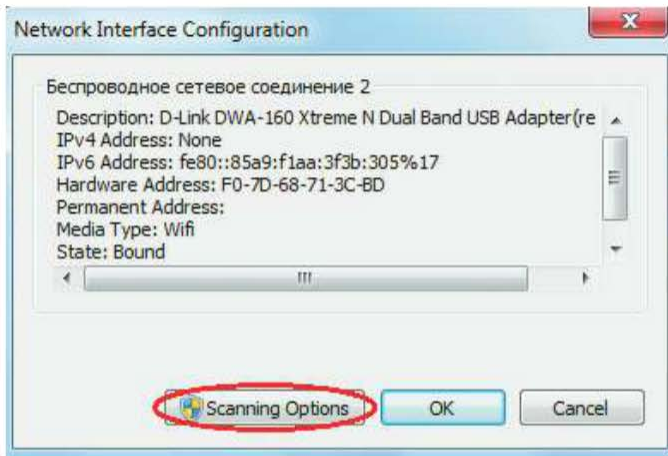


Рис. 4.7. Настройка беспроводного адаптера

В окне *WiFi Scanning Options* установите переключатель *Switch to Monitor Mode*, выберите *Select a layer and channel*, в выпадающем меню выберите *802.11n* и *6*. Нажмите кнопку *Apply* (рис. 4.8).

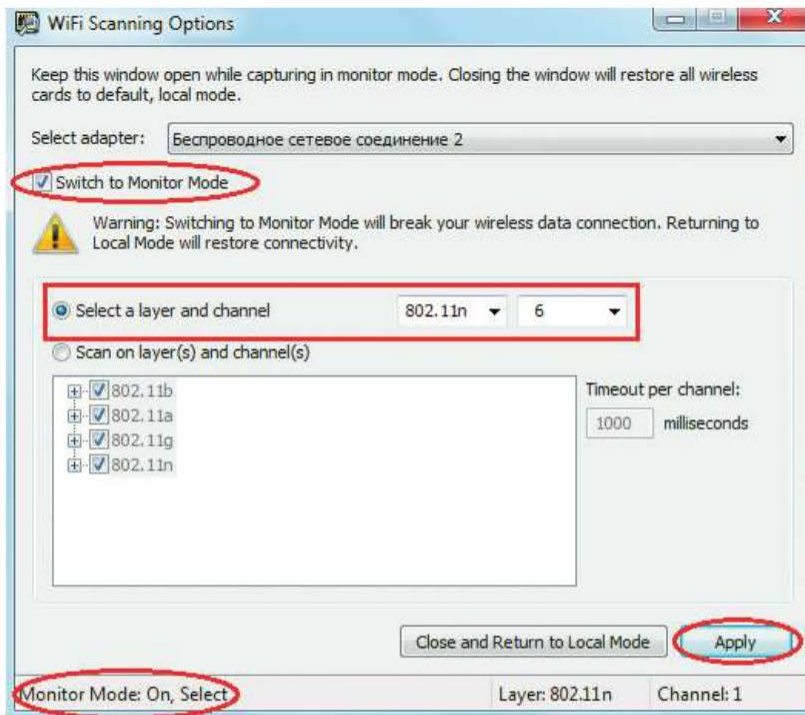


Рис. 4.8. Настройка беспроводного адаптера в режиме мониторинга

Примечание. Сверните окно *WiFi Scanning Options*. Если окно будет закрыто, функция мониторинга на беспроводном адаптере будет отключена автоматически.

Шаг 12. Запустите процесс захвата трафика, для чего нажмите кнопку *Start* на панели инструментов (рис. 4.9).

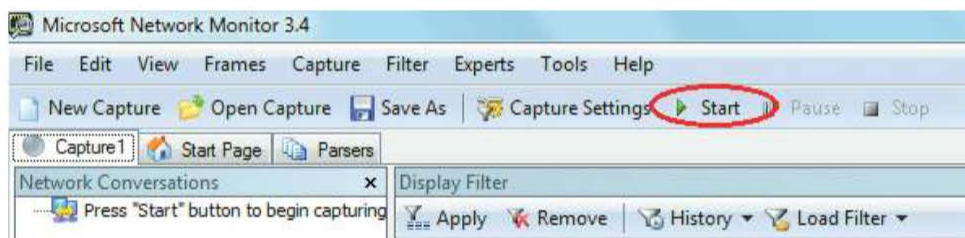


Рис. 4.9. Запуск процесса захвата кадров

Шаг 13. На рабочей станции ПК 2 подключитесь к беспроводной сети *class_N*. Зайдите на Web-интерфейс точки доступа. Отключитесь от беспроводной сети *class_N*.

Шаг 14. Остановите процесс захвата трафика, для чего нажмите кнопку *Stop* на панели инструментов.

Шаг 15. Сохраните захваченные кадры в файл. Для этого выберите меню *File* → *Save As...* В открывшемся окне введите имя файла и нажмите кнопку *Сохранить*.

4.2. Анализ кадров MAC стандарта IEEE 802.11

Шаг 1. Откройте файл с захваченными кадрами. Для этого выберите меню *File* → *Open* → *Capture* (рис. 4.10).

Шаг 2. Установите фильтр для отображения только *кадров данных* (Data frames). Для этого в окне *Display Filter* введите *WiFi.FrameControl.Type==2* и нажмите кнопку *Apply*. После применения фильтра в нижней части экрана можно посмотреть число кадров, подходящих под критерии фильтрации (Displayed), а также общее число перехваченных пакетов (Captured) (рис. 4.11).

Выберите один кадр данных в окне *Frame Summary*; при этом в окне *Frame Details* появится подробная информация о его структуре. В окне *Frame Details* выберите *WiFi* → *FrameControl* (рис. 4.12).

К какому подтипу относится захваченный кадр? _____

Проанализируйте захваченные кадры данных. Какие подтипы кадра данных встречаются чаще всего? _____

Какой процент составляют кадры данных от общего числа захваченных кадров? _____

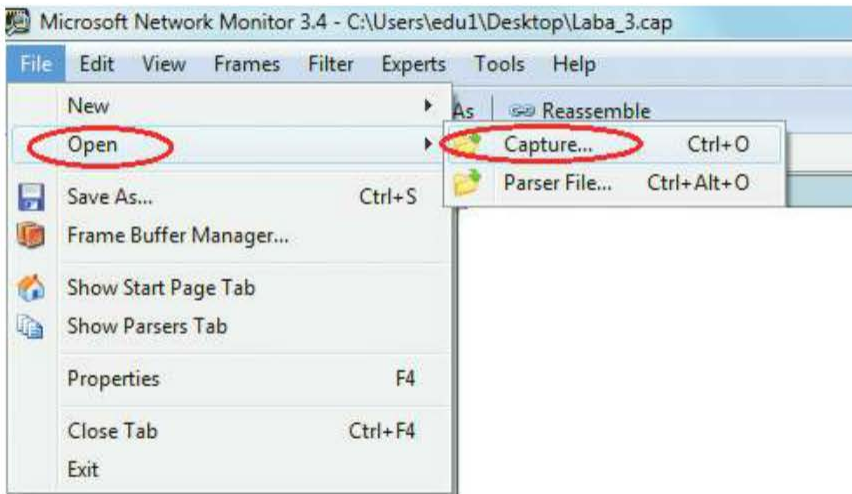


Рис. 4.10. Доступ к файлу с захваченными кадрами

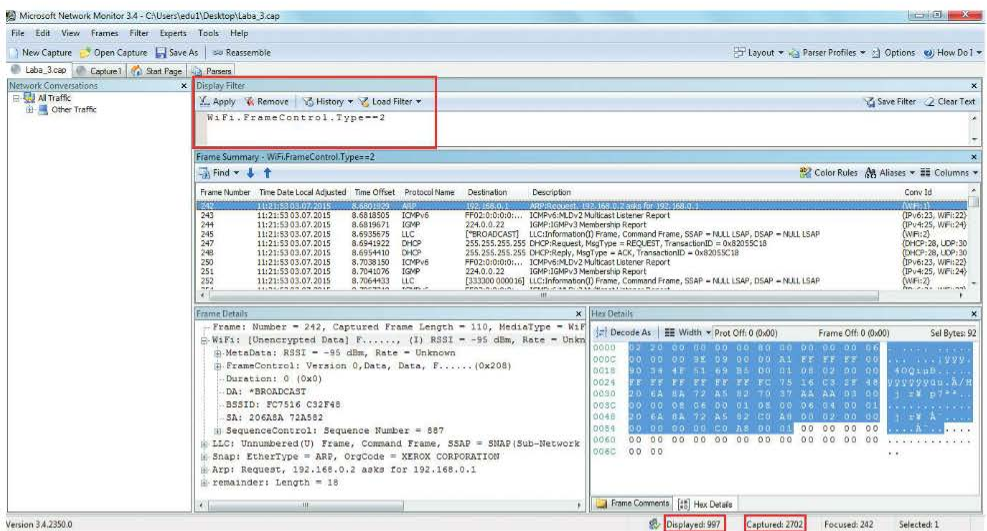


Рис. 4.11. Создание фильтра для отображения кадров данных

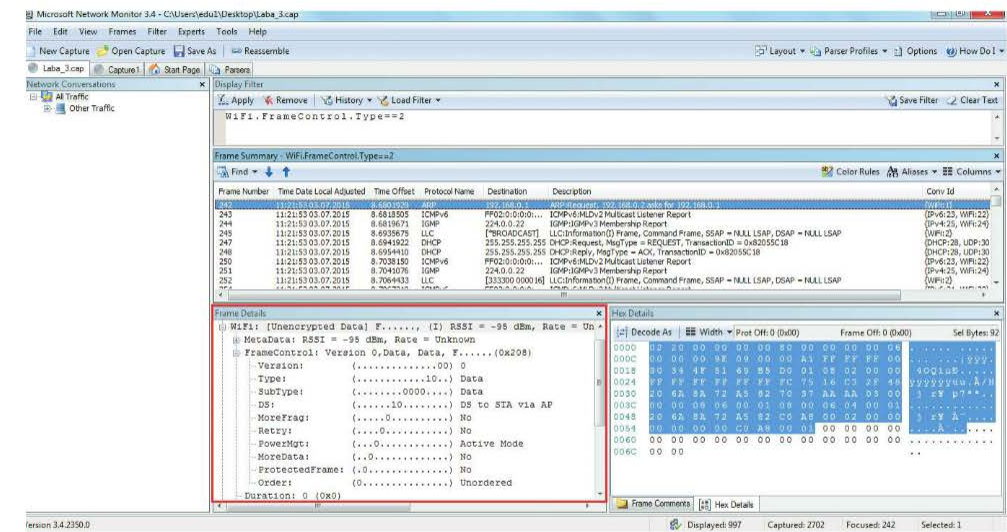


Рис. 4.12. Подробная информация о захваченном кадре данных

Шаг 3. Просмотрите количество повторно переданных кадров данных. Для этого установите фильтр *Wi-Fi.FrameControl.Type==2 && Wi-Fi.FrameControl.Retry==1* и нажмите кнопку *Apply* (рис. 4.13).

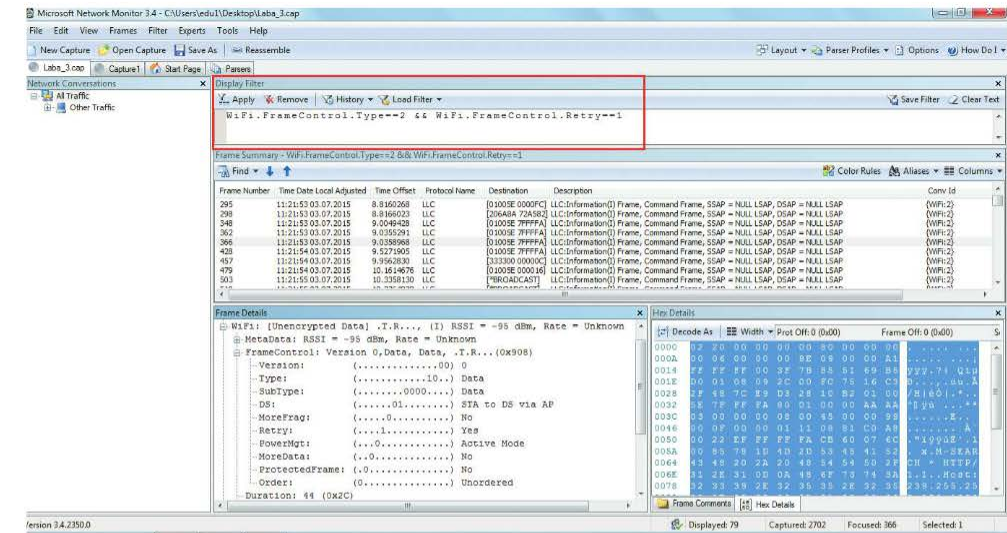


Рис. 4.13. Создание фильтра для просмотра повторно переданных кадров

П р и м е ч а н и е . Если кадр данных или кадр управления являются повторными, значения полей *Retry* равно 1. Каков процент повторно переданных кадров?

Шаг 4. Исследуйте контрольные кадры (Control frames). Для этого установите фильтр *WiFi.FrameControl.Type==1* и нажмите кнопку *Apply*.

Какой подтип контрольных кадров является самым распространенным из захваченных кадров? _____

Какой процент составляют контрольные кадры от общего числа захваченных кадров? _____

Шаг 5. Проанализируйте кадры управления (Management frames). Для этого установите фильтр *WiFi.FrameControl.Type==0* и нажмите кнопку *Apply*.

Какой подтип кадров управления является самым распространенным из захваченных кадров? _____

Какой процент составляют кадры управления от общего числа захваченных кадров? _____

Шаг 6. Выберите сигнальный кадр (Beacon) с SSID *class_N*. Для этого установите фильтр *WiFi.FrameControl.Type==0 && WiFi.FrameControl.SubType==8 && Property.WiFiSSIDValue=="class_N"*. Нажмите кнопку *Apply*. Разверните информацию со структурой кадра (рис. 4.14).

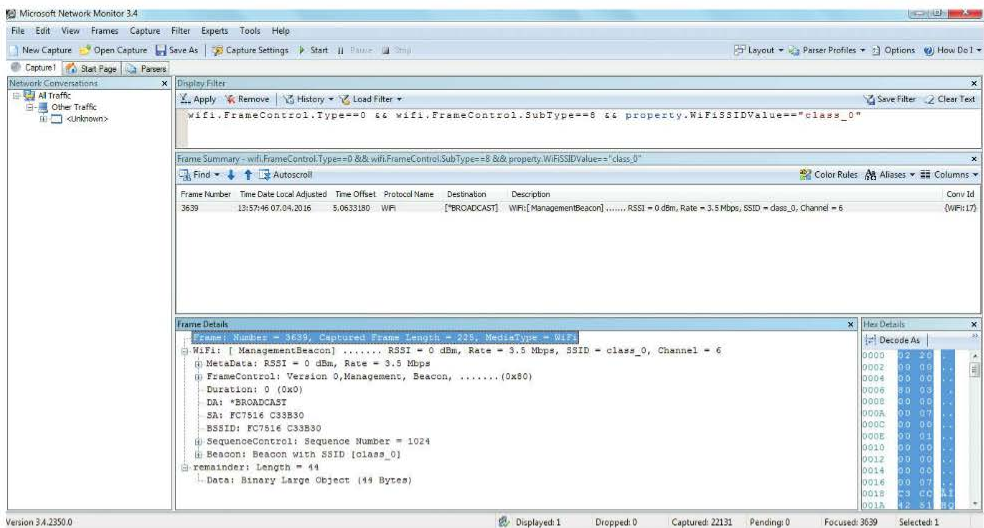


Рис. 4.14. Создание фильтра для просмотра сигнальных кадров (Beacon)

Примечание. Сигнальные кадры отправляются через определенные интервалы и содержат информацию о функциональных возможностях точки доступа, поддерживаемых скоростях, значении SSID, политиках безопасности.

Запишите идентификатор BSSID _____

Чем BSSID отличается от SSID? _____

Через сколько миллисекунд точка доступа рассылает сигнальные кадры?
В окне *Frame Details* выберите *WiFi* → *Beacon* → *BeaconInterval*
Какие скорости передачи поддерживает точка доступа?
Выберите *WiFi* → *Beacon* → *InformationElements* → *rates*

С какой скоростью точка доступа рассылает сигнальные кадры?
Выберите *WiFi* → *MetaData*

Шаг 7. Выберите кадр пробного запроса (Probe request) с SSID *class_N*. Для этого установите фильтр *WiFi.FrameControl.Type==0 && WiFi.FrameControl.SubType==4 && Property.WiFiSSIDValue=="class_N"*. Нажмите кнопку *Apply*. Разверните информацию со структурой кадра (рис. 4.15).

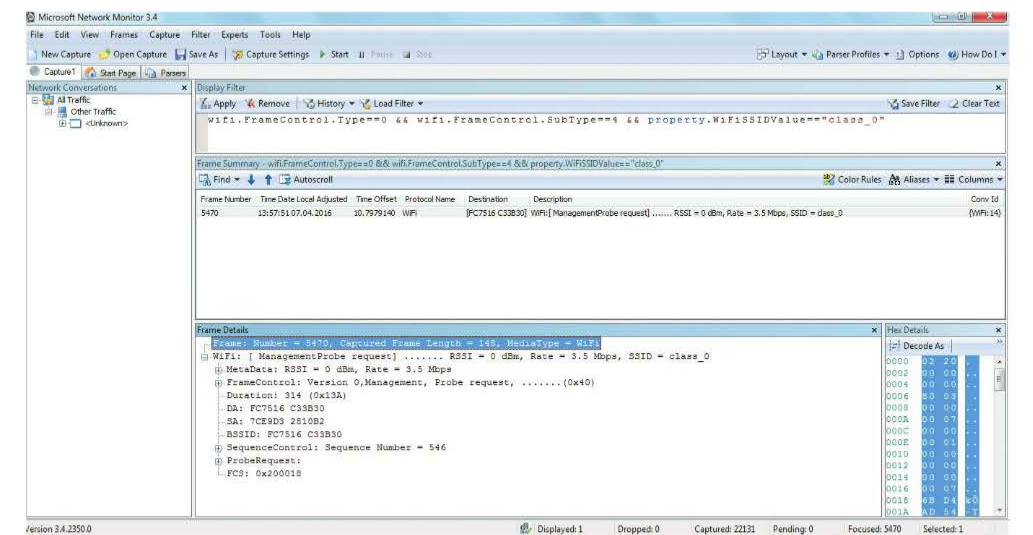


Рис. 4.15. Кадр пробного запроса

П р и м е ч а н и е . При активном сканировании станция последовательно отправляет широкоэвещательные кадры пробного запроса в каждый из проверяемых каналов. Пробный запрос содержит такую информацию, как поддерживаемые скорости передачи и стандарты, значение SSID.
Запишите идентификатор BSSID. Сравните его с BSSID сигнального кадра. Объясните различия

Какие скорости передачи поддерживает станция?
Выберите *WiFi* → *ProbeRequest* → *InformationElements* → *rates*

Шаг 8. Выберите кадр ответа на пробный запрос (Probe response) с SSID *class_N*. Для этого установите фильтр *WiFi.FrameControl.Type==0 && WiFi.FrameControl.SubType==5 && Property.WiFiSSIDValue=="class_N"*. Нажмите кнопку *Apply*. Разверните информацию со структурой кадра (рис. 4.16).

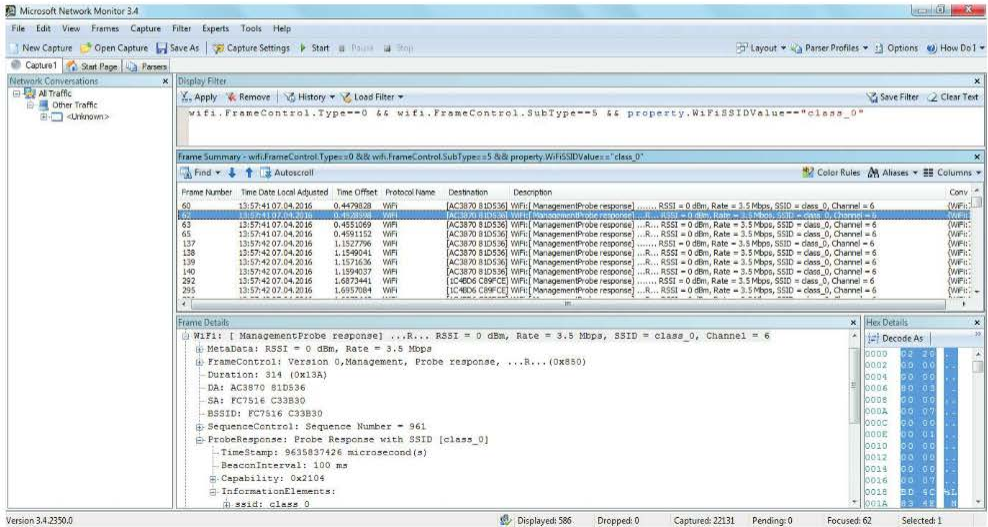


Рис. 4.16. Кадр ответа на пробный запрос

Примечание. Точка доступа отвечает на пробный запрос в том случае, если значение SSID в поступившем запросе совпадает с ее собственным. Ответ на пробный запрос содержит информацию о SSID, поддерживаемых скоростях передачи, типах шифрования и других возможностях точки доступа.

Какие скорости передачи поддерживает точка доступа?
Выберите *WiFi* → *ProbeResponse* → *InformationElements* → *rate*

Шаг 9. Установите фильтр для отображения кадров аутентификации (Authentication). Для этого в окне *Display Filter* введите *WiFi.FrameControl.Type==0 && WiFi.FrameControl.SubType==11*. Нажмите кнопку *Apply* (рис. 4.17, 4.18).

Примечание. При аутентификации открытых систем (Open system) станция, инициировавшая процесс аутентификации, отправляет точке доступа кадр аутентификации с номером последовательности 0x0001, содержащий запрос аутентификации.

Примечание. При аутентификации открытых систем (Open system) точка доступа отвечает станции кадром аутентификации с номером последовательности 0x0002. В случае успешной аутентификации код состояния в кадре «successful».

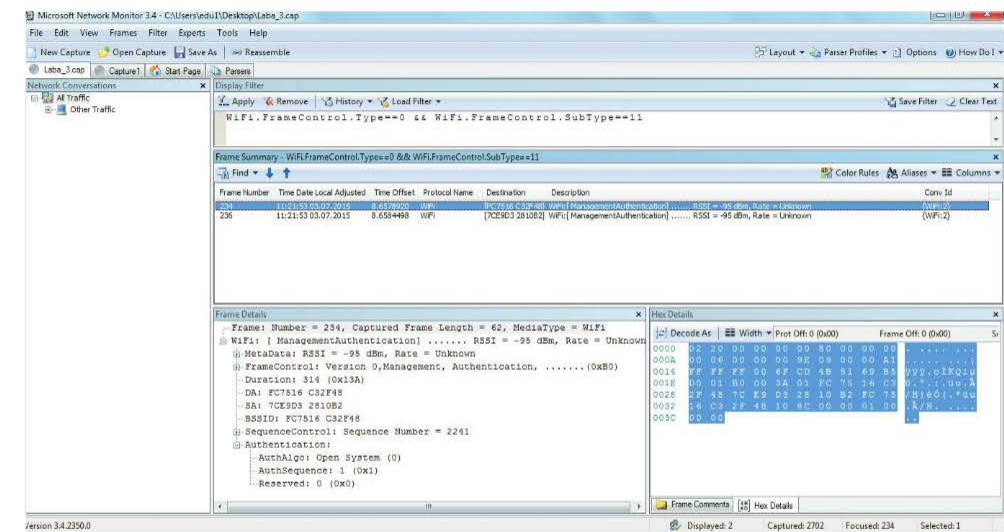


Рис. 4.17. Кадр запроса аутентификации со стороны клиента

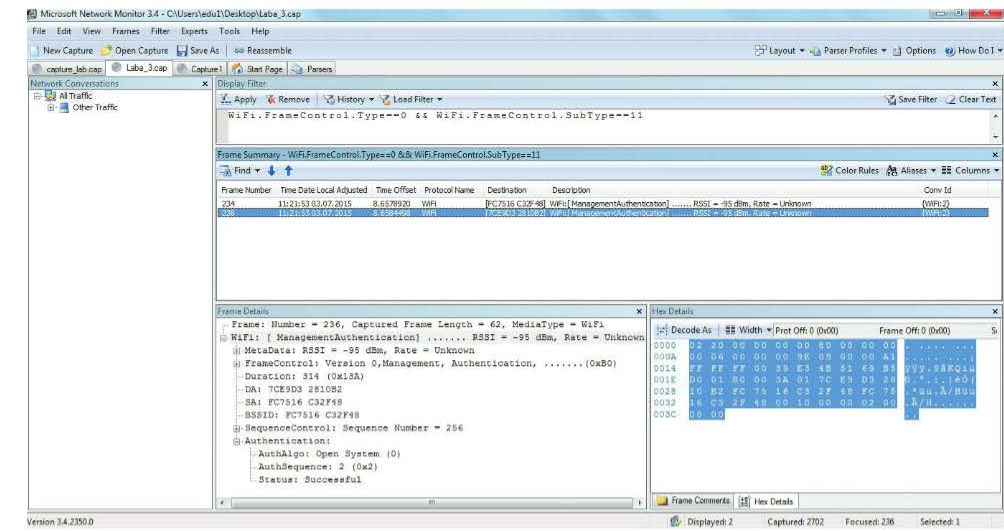


Рис. 4.18. Кадр ответа на запрос аутентификации

Шаг 10. Выберите кадр запроса ассоциации (Association request). Для этого установите фильтр `WiFi.FrameControl.Type==0 && WiFi.FrameControl.SubType==0`. Нажмите кнопку *Apply*. Разверните информацию со структурой кадра (рис. 4.19).

Примечание. После успешной аутентификации станция отправляет точке доступа запрос ассоциации, содержащий информацию о своих возможностях.

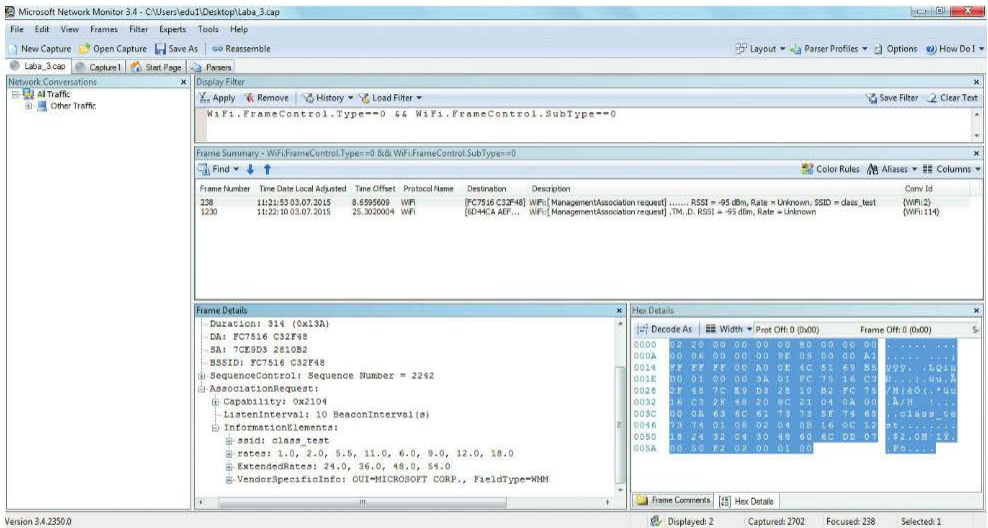


Рис. 4.19. Кадр запроса на ассоциацию

Какие скорости передачи поддерживает станция?

Выберите *WiFi* → *AssociationRequest* → *InformationElements* → *rates*

Шаг 11. Выберите кадр ответа на запрос ассоциации (Association response). Установите фильтр *WiFi.FrameControl.Type==0 && WiFi.FrameControl.SubType==1* и нажмите кнопку *Apply*. Разверните информацию со структурой кадра (рис. 4.20).

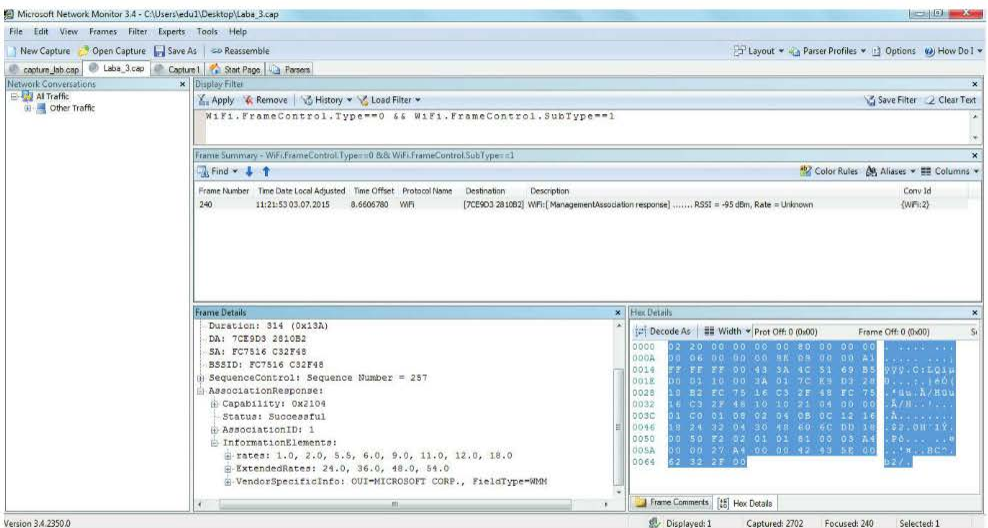


Рис. 4.20. Кадр ответа на запрос ассоциации

Примечание. Точка доступа получает запрос и проверяет, совпадают ли ее возможности с возможностями станции, и если они совпадают, точка создает для станции идентификатор ассоциации (association identifier, AID) и отправляет ей ответ на запрос ассоциации, содержащий код состояния «successful».

Запишите идентификатор ассоциации *WiFi* → *AssociationResponse* _____

Лабораторная работа № 5. Изучение пассивного и активного сканирования

Для работы беспроводных устройств выделены определенные частотные диапазоны. Каждый диапазон, в свою очередь, делится на каналы (*channel*), количество и ширина которых зависят от используемой на физическом уровне 802.11 технологии. Каналы необходимы для взаимодействия беспроводных устройств друг с другом.

Как только точка доступа переходит в активное состояние, она через определенные временные интервалы начинает широковещательно отправлять в каждый канал сигнальные кадры (Beacon), содержащие информацию о функциональных возможностях точки доступа, поддерживаемых скоростях, значении SSID, политиках безопасности.

До начала работы на точке доступа и станциях должны быть настроены все параметры, требуемые для нормального функционирования сети.

Перед подключением к точке доступа беспроводной клиент проводит активное или пассивное сканирование каждого канала с целью определения доступных сетей (точек доступа). В ходе пассивного сканирования станция в течение определенного периода времени прослушивает каждый канал на предмет обнаружения передаваемых точками доступа сигнальных кадров. По содержащейся в них информации о SSID и определяются доступные для подключения беспроводные сети.

При активном сканировании клиент последовательно отправляет широковещательные кадры пробного запроса (*Probe request*) в каждый из проверяемых каналов. Пробный запрос содержит информацию о скорости передачи, поддерживаемых стандартах и значении SSID. Для того чтобы все точки доступа могли получить запрос, в качестве адреса назначения и идентификатора BSSID указывается широковещательный адрес FF:FF:FF:FF:FF:FF. Точка доступа отвечает на пробный запрос в том случае, если значение SSID в поступившем запросе совпадает с ее собственным либо является wildcard SSID (SSID нулевой длины, означающий «все SSID»). Ответ на пробный запрос (*Probe response*) содержит информацию о SSID, поддерживаемых скоростях передачи, типах шифрования и других возможностях точки доступа. Ответ посылается на индивидуальный адрес станции, отправившей запрос.

Клиент может получить ответ на пробный запрос (*Probe response*) от нескольких точек доступа большой сети и должен выбрать, к какой из них подключиться. Механизм, по которому клиент выбирает точку доступа для ассо-

циации с ней, не описан в стандарте IEEE 802.11 и реализуется производителями оборудования самостоятельно. В общем случае критерий выбора точки доступа может быть основан на SSID, уровне сигналов, совместимых типах шифрования и аутентификации, собственных критериях производителя.

Оборудование (на 1 рабочее место):

Рабочая станция	2 шт.
Беспроводной адаптер DWA-160 или DWA-582	2 шт.
Точка доступа DAP-2310	1 шт.
Кабель Ethernet	1 шт.
ПО — анализатор трафика Microsoft Network Monitor 3.4.	

Цель работы: исследование процессов пассивного и активного сканирования.

Перед выполнением задания (рис. 5.1) верните настройки точки доступа к заводским настройкам по умолчанию.



Рис. 5.1. Схема сети

Примечание. Настройка точки доступа выполняется с рабочей станции ПК 1.

Шаг 1. Подключите Ethernet-кабель к LAN-порту точки доступа и к сетевому адаптеру рабочей станции ПК 1.

Шаг 2. Настройте статический IP-адрес на Ethernet-адаптере рабочей станции ПК 1 — 192.168.0.1 с маской подсети 255.255.255.0.

Шаг 3. Зайдите на Web-интерфейс точки доступа. Измените IP-адрес управления на 192.168.N.50 с маской подсети 255.255.255.0. Сохраните и активируйте настройки.

Шаг 4. Измените IP-адрес Ethernet-адаптера рабочей станции ПК1 на 192.168.N.1 с маской подсети 255.255.255.0.

Шаг 5. Уменьшите выходную мощность передатчика точки доступа до 12,5 %.

Шаг 6. Создайте беспроводную сеть с SSID *Dlink_N*, для чего:

- 1) выберите раздел *Basic Settings* → *Wireless*;
- 2) в списке *Mode* выберите *Access Point*;
- 3) в поле *Network Name (SSID)* введите *Dlink_N*;
- 4) отключите автоматический выбор канала. Для этого в поле *Auto Channel Selection* выберите *Disable*;
- 5) в поле *Channel* выберите 6;
- 6) в выпадающем меню *Authentication* выберите *Open System*;
- 7) сохраните настройки, нажав кнопку *Save*.

Шаг 7. Сохраните и активируйте настройки. Для этого выберите *Configuration* → *Save and Activate*.

Шаг 8. Отключите Ethernet-кабель от точки доступа.

Шаг 9. Настройте на беспроводных интерфейсах ПК 1 и ПК 2 статические IP-адреса в соответствии с рис. 5.1 и номером рабочей группы.

Шаг 10. Просмотрите MAC-адрес беспроводного адаптера ПК 2. В командной строке введите: `getmac`

MAC-адрес ПК 2 _____

Шаг 11. Запустите на рабочей станции ПК 1 анализатор протоколов Microsoft Network Monitor. Выберите интерфейс, с которого будет выполняться перехват трафика, и активируйте функцию мониторинга на беспроводном адаптере. Процесс активации функции мониторинга описан в лабораторной работе № 4.

Примечание. В окне WiFi Scanning Options установите переключатель Switch to Monitor Mode, выберите Scan on layer(s) and channel(s) и поставьте галочки для спецификаций 802.11b, 802.11a, 802.11g и 802.11n. Нажмите кнопку Apply.

Шаг 12. Запустите захват трафика. Для этого нажмите кнопку *Start* на панели инструментов. Подождите несколько минут, пока не будет захвачено достаточное для анализа количество кадров.

Шаг 13. Остановите захват трафика. Для этого нажмите кнопку *Stop* на панели инструментов. Проанализируйте захваченные кадры.

Шаг 14. Проверьте, рассылает ли точка доступа сигнальные кадры о сети с SSID *Dlink_N*. Для этого установите фильтр *WiFi.FrameControl.Type==0 && WiFi.FrameControl.SubType==8 && property.WiFiSSIDValue=="Dlink_N"* и нажмите *Apply* (рис. 5.2).

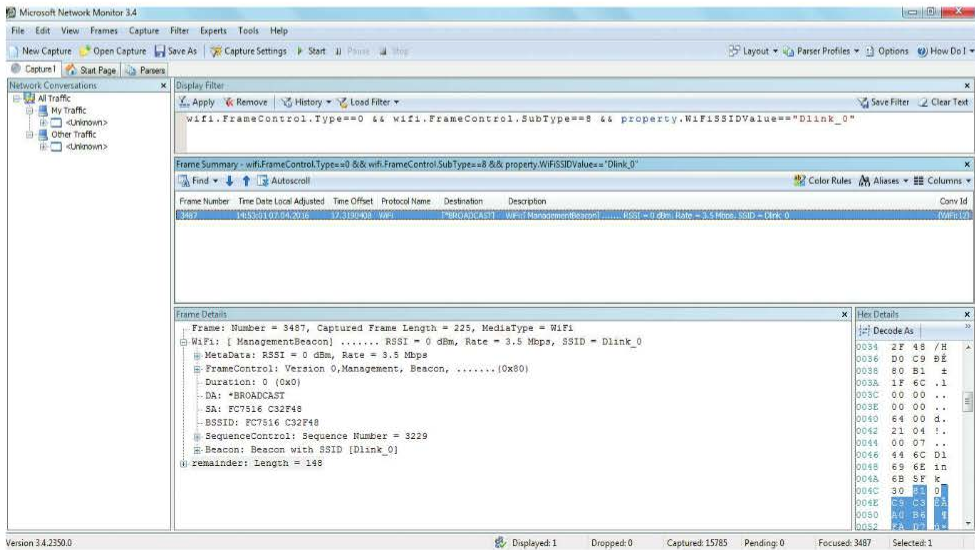


Рис. 5.2. Сигнальный кадр

Запишите MAC-адрес источника (SA) _____

Сравните MAC-адрес источника с MAC-адресом, указанным на точке доступа (наклейка на задней панели устройства).

Запишите MAC-адрес назначения (DA) в шестнадцатеричном виде _____

Запишите BSSID _____

Шаг 15. Просмотрите кадры пробного запроса (Probe request), отправленные рабочей станцией ПК 2. Для этого установите фильтр *WiFi.FrameControl.Type==0 && WiFi.FrameControl.SubType==4 && WiFi.Management.SA==0x7ce9d32810b2* и нажмите кнопку *Apply*. Разверните информацию со структурой кадра (рис. 5.3).

Примечание. Вместо 0x7ce9d32810b2 введите реальный MAC-адрес беспроводного интерфейса ПК 2.

Какой идентификатор SSID указан в пробном запросе? _____

Какой адрес указан в полях DA и BSSID? _____

используются протоколы TKIP и CCMP. Программы сертификации WPA/WPA2 основаны на IEEE 802.11i и определяют набор функций безопасности, которые должны присутствовать в производимом оборудовании для обеспечения безопасности беспроводных сетей. В зависимости от требований сети WPA/WPA2 работают в одном из двух режимов — Enterprise и Personal. Режим Personal основан на аутентификации PSK, режим Enterprise — на аутентификации на основе стандарта IEEE 802.1X. В WPA для обеспечения конфиденциальности данных используется протокол TKIP, в WPA2 — протокол CCMP.

Информация о функциях безопасности станции или точки доступа указывается в элементе RSN IE кадров Beacon, Probe response, Association request.

В беспроводных сетях могут использоваться механизмы контроля доступа, выходящие за рамки стандарта IEEE 802.11. Контроль над подключением клиента к точке доступа на основе его MAC-адреса не предусмотрен стандартом IEEE 802.11, однако поддерживается многими производителями оборудования для беспроводных сетей, в том числе D-Link. Для этого точка доступа должна поддерживать функцию фильтрации по MAC-адресам (MAC Filtering), которая позволяет разрешать или запрещать подключение клиентов к сети на основе их MAC-адресов. Сетевой администратор может настроить на точке доступа список разрешенных или запрещенных MAC-адресов. При попытке подключения беспроводного клиента точка доступа проверяет заранее настроенный список и определяет, разрешено ли этому клиенту подключаться к сети или нет. Функция фильтрации по MAC-адресам может использоваться совместно с механизмами аутентификации, например открытой аутентификацией или аутентификацией с общим ключом.

Оборудование (на 1 рабочее место):

Рабочая станция	2 шт.
Беспроводной адаптер DWA-160 или DWA-582	2 шт.
Точка доступа DAP-2310	1 шт.
Кабель Ethernet	1 шт.
ПО — анализатор трафика Microsoft Network Monitor 3.4.	

Цель работы: изучить настройку режима WPA/WPA2-Personal и принцип работы фильтрации по MAC-адресам.

6.1. Настройка режима WPA/WPA2-Personal

Перед выполнением задания (рис. 6.1) верните настройки точки доступа к заводским настройкам по умолчанию.

Примечание. Настройка точки доступа выполняется с рабочей станции ПК 1.

Шаг 1. Подключите Ethernet-кабель к LAN-порту точки доступа и к сетевому адаптеру рабочей станции ПК 1.

Шаг 2. Настройте статический IP-адрес на Ethernet-адаптере рабочей станции ПК 1 — 192.168.0.1 с маской подсети 255.255.255.0.



Рис. 6.1. Схема сети

Шаг 3. Зайдите на Web-интерфейс точки доступа. Измените IP-адрес управления на 192.168.N.50 с маской подсети 255.255.255.0. Сохраните и активируйте настройки.

Шаг 4. Измените IP-адрес Ethernet-адаптера рабочей станции ПК 1 на 192.168.N.1 с маской подсети 255.255.255.0.

Шаг 5. Уменьшите выходную мощность передатчика точки доступа до 12,5 %.

Шаг 6. Создайте беспроводную сеть с SSID *Dlink_N* и настройте режим WPA/WPA2-Personal (рис. 6.2). Для этого:

- 1) выберите раздел *Basic Settings* → *Wireless*;
- 2) в списке *Mode* выберите *Access Point*;
- 3) в поле *Network Name (SSID)* введите *Dlink_N*;
- 4) отключите автоматический выбор канала. Для этого в поле *Auto Channel Selection* выберите *Disable*;
- 5) в поле *Channel* выберите 6;
- 6) в выпадающем меню *Authentication* выберите *WPA-Personal*;



Рис. 6.2. Окно настройки WPA/WPA2-Personal

- 7) в списке *WPA Mode* выберите *AUTO (WPA or WPA2)*;
- 8) в списке *Cipher Type* выберите *AES*;
- 9) в поле *PassPhrase* введите пароль *DlinkPassword*;
- 10) в поле *Confirm PassPhrase* повторите пароль *DlinkPassword*;
- 11) сохраните настройки, нажав кнопку *Save*.

Шаг 7. Сохраните и активируйте настройки. Для этого выберите *Configuration* → *Save and Activate*.

Шаг 8. Отключите Ethernet-кабель от точки доступа.

Шаг 9. Настройте на беспроводных интерфейсах ПК 1 и ПК 2 статические IP-адреса в соответствии с рис. 6.1 и номером рабочей группы.

Шаг 10. Запустите на рабочей станции ПК 1 анализатор протоколов Microsoft Network Monitor. Выберите интерфейс, с которого будет выполняться перехват трафика, и активируйте функцию мониторинга на беспроводном адаптере.

Шаг 11. Запустите процесс захвата трафика. Для этого нажмите кнопку *Start* на панели инструментов.

6.2 Контроль доступа к беспроводной сети на основе MAC-адресов

Шаг 1. Посмотрите MAC-адреса беспроводных интерфейсов ПК 1 и ПК 2. В командной строке введите: `getmac`

MAC-адрес ПК 1 _____

MAC-адрес ПК 2 _____

Шаг 2. Подключите рабочую станцию ПК 1 к точке доступа Ethernet-кабелем. Зайдите на Web-интерфейс. Выберите *Advanced Settings* → *Filters* → *Wireless MAC ACL*. Включите фильтрацию подключений к точке доступа по MAC-адресам — в поле *Access Control List* выберите *Accept*. В поле *MAC Address* введите MAC-адрес рабочей станции ПК 2 и нажмите кнопки *Add* и *Save* (рис. 6.4).

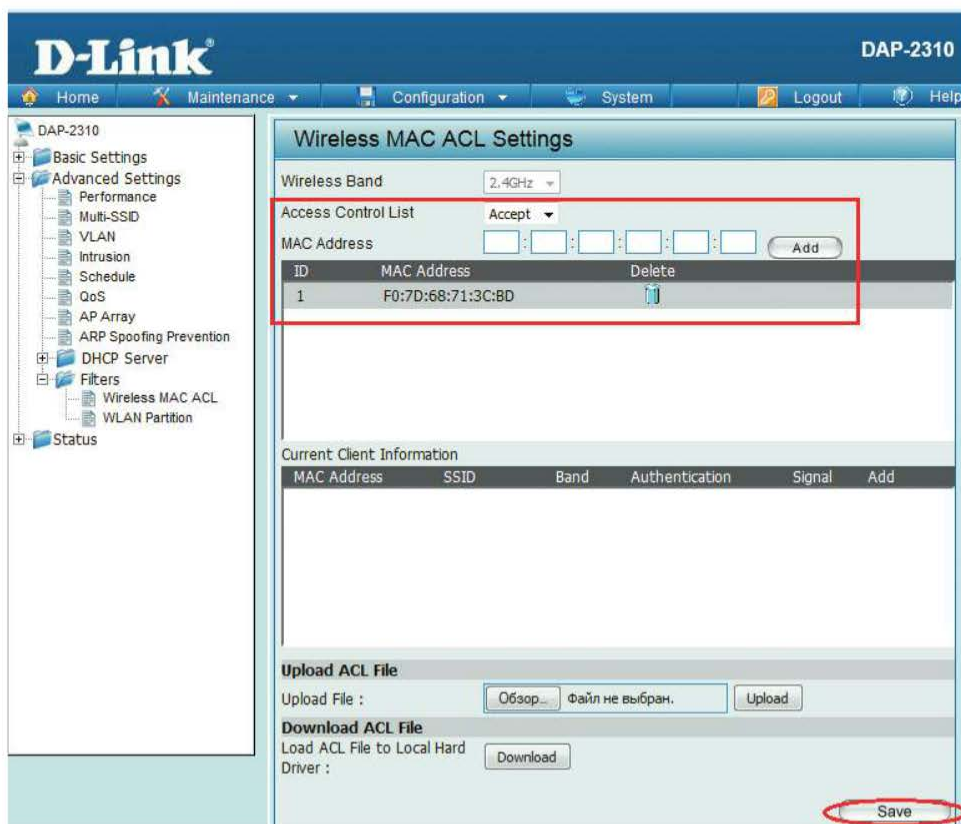


Рис. 6.4. Настройка фильтрации по MAC-адресам по типу «белого списка»

Примечание. Включенный фильтр действует по типу «белого списка»: ассоциироваться с точкой доступа будет разрешено только устройствам, MAC-адреса которых содержатся в списке.

Шаг 3. Сохраните и активируйте настройки.

Шаг 4. Отключите Ethernet-кабель от точки доступа.

Шаг 5. Подключитесь на рабочих станциях ПК 1 и ПК 2 к беспроводной сети *Dlink_N*.

Произошла ассоциация рабочей станции ПК 1 с точкой доступа? _____

Произошла ассоциация рабочей станции ПК 2 с точкой доступа? _____

Шаг 6. На рабочей станции ПК 1 зайдите на Web-интерфейс точки доступа. Выберите *Advanced Settings* → *Filters* → *Wireless MAC ACL*. Измените фильтр на запрещающий — в поле *Access Control List* выберите *Reject* и нажмите кнопку *Save* (рис. 6.5).

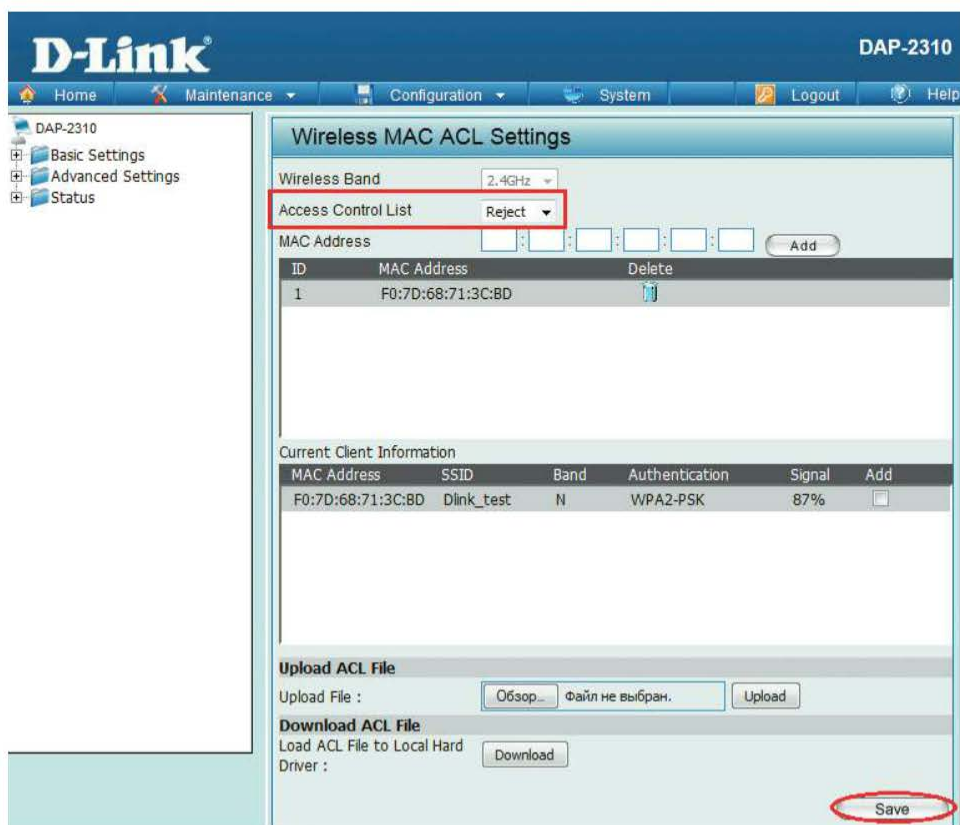


Рис. 6.5. Настройка фильтрации по MAC-адресам по типу «черного списка»

Примечание. Настроенный фильтр действует по типу «черного списка»: ассоциироваться с точкой доступа будет разрешено всем устройствам, кроме тех, чьи MAC-адреса содержатся в списке.

Шаг 7. Сохраните и активируйте настройки.

Шаг 8. Подключитесь на рабочих станциях ПК 1 и ПК 2 к беспроводной сети *Dlink_N*.

Произошла ассоциация рабочей станции ПК 1 с точкой доступа? _____

Произошла ассоциация рабочей станции ПК 2 с точкой доступа? _____

Шаг 9. Отключите фильтрацию подключений к точке доступа по MAC-адресам. Выберите *Advanced Settings* → *Filters* → *Wireless MAC ACL*. В поле *Access Control List* выберите *Disable* и нажмите кнопку *Save*.

Шаг 10. Сохраните и активируйте настройки.

Шаг 11. Подключитесь на рабочих станциях ПК 1 и ПК 2 к беспроводной сети *Dlink_N*.

Произошла ассоциация рабочей станции ПК 1 с точкой доступа? _____

Произошла ассоциация рабочей станции ПК 2 с точкой доступа? _____

Лабораторная работа № 7. Расчет беспроводной линии связи

Проектирование беспроводных сетей практически невозможно без оценки пригодности линии связи, позволяющей выявить возможные проблемы в ходе их установки. Наличие хорошего энергетического потенциала является базовым условием для нормального функционирования линии связи.

Энергетический потенциал (*Link budget*) беспроводной линии связи учитывает все усиления и потери уровня сигнала при его распространении от передатчика к приемнику через беспроводную среду передачи, кабели, разъемы и различные препятствия (стены, потолки, деревья и т. д.).

Полное уравнение энергетического потенциала линии связи можно записать следующим образом:

$$P_{tr} - L_{tr} + G_{tr} - L_{bf} + G_{recv} - L_{rcv} = SOM + P_{recv}, \quad (Л7.1)$$

где P_{tr} — мощность передатчика, дБм (dBm); L_{tr} — потери сигнала в антенном кабеле и разъемах передающего тракта, дБ (dB); G_{tr} — коэффициент усиления передающей антенны, дБ (dBi); L_{bf} — потери в свободном пространстве, дБ (dB); G_{recv} — коэффициент усиления приемной антенны, дБ (dBi); L_{rcv} — потери сигнала в антенном кабеле и разъемах приемного тракта, дБ (dB); SOM — запас на замирание сигнала (SOM, System Operating Margin), дБ (dB); P_{recv} — чувствительность приемника при данной скорости передачи, дБм (dBm).

Потери в свободном пространстве для линии связи с изотропными антеннами можно рассчитать с помощью следующей формулы:

$$L_{bf} = 20 \lg F + 20 \lg D + K, \quad (Л7.2)$$

где L_{bf} — потери в свободном пространстве; F — центральная частота канала, на котором работает система связи; D — расстояние между двумя антеннами; K — константа, которая зависит от единиц измерения частоты и расстояния:

- для частоты, выраженной в ГГц, и расстояния, измеряемого в километрах, константа равна 92,45;
- для частоты, выраженной в МГц, и расстояния, измеряемого в километрах, константа равна 32,4;
- для частоты, выраженной в МГц, и расстояния, измеряемого в метрах, константа равна $-27,55$.

Для других типов антенн следует учитывать коэффициент усиления. В результате выражение для потерь в свободном пространстве примет следующий вид:

$$L_{bf} = 20 \lg F + 20 \lg D - G_{tr} - G_{recv} + K, \quad (Л7.3)$$

где G_{tr} — коэффициент усиления передающей антенны; G_{recv} — коэффициент усиления приемной антенны.

Надежность работы беспроводной линии связи в первую очередь определяется энергетическим запасом на быстрые и медленные замирания. Поэтому при ее расчете обязательно должен быть предусмотрен резерв на компенсацию этих замираний — запас на замирание сигнала (SOM). SOM определяется как разница между уровнем фактически принимаемого сигнала и чувствительностью приемника, которая зависит от выбранного типа модуляции:

$$SOM = P_{tr} - L_{tr} + G_{tr} - L_{bf} + G_{recv} - L_{recv} - P_{recv}. \quad (Л7.4)$$

Чем выше SOM, тем надежнее беспроводная линия связи. Считается, что минимальная величина запаса на замирание должна быть не меньше 10 дБ и этого достаточно для инженерного расчета, но на практике зачастую используют значение 20...30 дБ.

Для обеспечения эффективной связи с помощью сантиметровых волн необходимо обеспечить линию прямой видимости между передатчиком и приемником. Однако это не всегда возможно, особенно при построении беспроводных сетей вне помещений. Для определения объема свободного от преград пространства на линии связи между передатчиком и приемником используется такое понятие, как зона Френеля (Fresnel zone).

Зона, ближайшая к линии, соединяющей передатчик с приемником, называется первой зоной Френеля. Все естественные (земля, холмы, деревья) и искусственные (здания, столбы) препятствия, попадающие в нее, оказывают наиболее негативное влияние на уровень сигнала в результате отражения, преломления, рассеивания или дифракции. При этом чем длиннее линия связи, тем важнее становится вычисление радиуса первой зоны Френеля.

Для любой точки радиолинии радиус первой зоны Френеля можно найти по формуле

$$R = 17,32 \sqrt{\frac{S_1 S_2}{F(S_1 + S_2)}}, \quad (\text{Л7.5})$$

где R — радиус первой зоны Френеля, м; S_1 — расстояние от антенны передатчика до самой высшей точки предполагаемого препятствия, км; S_2 — расстояние от самой высшей точки предполагаемого препятствия до антенны приемника, км; F — частота, ГГц.

Учитывая тот факт, что максимальный радиус первая зона Френеля имеет в точке, равноудаленной от обеих антенн, получим упрощенную формулу для его вычисления:

$$R = 17,32 \sqrt{\frac{D}{4F}}. \quad (\text{Л7.6})$$

Если в области, радиус которой составляет 60 % первой зоны Френеля, нет преград, то при расчете радиолинии можно ограничиться учетом потерь сигнала в свободном пространстве. Для достижения этого высота подвеса антенн приемника и передатчика должна быть такой, чтобы вдоль радиолинии не было ни одной точки, расстояние от которой до препятствия было бы меньше, чем 0,6 радиуса первой зоны Френеля. Следует отметить, что поверхность земли также является одним из препятствий.

Для упрощенного вычисления радиуса области, составляющего 60 % радиуса первой зоны Френеля, умножим выражение предыдущей формулы на коэффициент 0,6:

$$R(60) = 10,4 \sqrt{\frac{D}{4F}}. \quad (\text{Л 7.7})$$

При установке более жестких требований преграды должны отсутствовать в 80 % первой зоны Френеля. Для упрощенного вычисления радиуса области, составляющего 80 % радиуса первой зоны Френеля, нужно умножить выражение (Л7.6) на коэффициент 0,8:

$$R(80) = 13,86 \sqrt{\frac{D}{4F}}. \quad (\text{Л7.8})$$

Следует понимать, что радиус первой зоны Френеля не является высотой установки антенн, но используется для ее вычисления. Определяя высоту установки антенн, следует учитывать также кривизну земной поверхности, выраженную в м, которую можно рассчитать по формуле

$$H_{\text{earth}} = \frac{D^2}{68}. \quad (\text{Л7.9})$$

Минимальная высота установки антенн над препятствиями с учетом того, что 60 % первой зоны Френеля свободно от преград, будет вычисляться по формуле

$$H_{ant} = 10,4 \sqrt{\frac{D}{4F}} + \frac{D^2}{68}. \quad (\text{Л7.10})$$

Если необходимо рассчитать высоту установки антенны при отсутствии препятствий в 80 % первой зоны Френеля, то коэффициент 10,4 в формуле (Л7.10) надо заменить на 13,86.

Цель работы: научиться оценивать пригодность линии связи для выявления возможных проблем в ходе установки беспроводного оборудования.

7.1. Примеры расчета беспроводной линии связи

ПРИМЕР 1

Оцените возможность работы канала связи длиной 2 км между точкой доступа DAP-3310 и беспроводным клиентом с адаптером DWA-182 на максимальной скорости, поддерживаемой беспроводной сетью (300 Мбит/с). Устройства работают на 6 канале (центральная частота 2437 МГц).

РЕШЕНИЕ

Запишем технические характеристики DAP-3310 и DWA-182:

- мощность передатчика на всех скоростях DAP-3310: 20 dBm;
- мощность передатчика DWA-182 на скорости 300 Мбит/с: 15 dBm;
- мощность передатчика DWA-182 на скорости 1 Мбит/с: 19 dBm;
- чувствительность DAP-3310 на скорости 300 Мбит/с: -69 dBm;
- чувствительность DAP-3310 на скорости 1 Мбит/с: -96 dBm;
- чувствительность DWA-182 на скорости 300 Мбит/с: -61 dBm;
- чувствительность DWA-182 на скорости 1 Мбит/с: -87 dBm;
- коэффициент усиления штатной антенны DAP-3310: 10 dBi;
- коэффициент усиления штатной антенны DWA-182: 0 dBi;
- потерь в антенно-фидерном тракте, т. е. между беспроводными устройствами и их антеннами, нет (0 дБм).

Примечание. Характеристики устройств можно посмотреть на сайте <http://dlink.ru> → *Продукты и решения* → *Беспроводное оборудование*. Далее необходимо перейти на страницу DAP-3310 и DWA-182 в раздел *Характеристики*.

Шаг 1. Оценим линию связи в направлении от точки доступа к клиенту. Найдем потери в свободном пространстве по формуле (7.2):

$$20 \lg(2437) + 20 \lg(2) + 32,4 = 106,2 \text{ дБ.}$$

Рассчитаем запас на замирание для скорости 300 Мбит/с по формуле (7.4):

$$SOM = 20 - 0 + 10 - 106,2 + 0 - 0 - (-61) = -15,2 \text{ дБ.}$$

Шаг 2. Оценим линию связи в обратном направлении — от клиента к точке доступа.

Рассчитаем запас на замирание по формуле (7.4):

$$SOM = 15 - 0 + 0 - 106,2 + 10 - 0 - (-69) = -12,2 \text{ дБ.}$$

Вывод: запас на замирание линии связи в обоих направлениях намного меньше 10 дБм, что говорит о ее недостаточном энергетическом потенциале.

ПРИМЕР 2

Определите максимальное расстояние, на котором линия связи между DAP-3310 и DWA-182 будет стабильно работать в обоих направлениях при скоростях передачи 300 Мбит/с и 1 Мбит/с.

РЕШЕНИЕ

Формула для расчета дальности связи выводится из выражения для потерь в свободном пространстве:

$$D = 10^{\left(\frac{L_{bf} - 20 \lg F - K}{20} \right)}. \quad (\text{Л7.11})$$

Исходя из полного уравнения энергетического потенциала линии связи, потери в свободном пространстве можно вычислить следующим образом:

$$L_{bf} = P_{tr} - L_{tr} + G_{tr} + G_{recv} - L_{recv} - P_{recv} - SOM. \quad (\text{Л7.12})$$

Шаг 1. Найдем расстояние между устройствами при передаче данных на скорости 300 Мбит/с. Передающее устройство — DAP-3310, принимающее устройство — DWA-182. Значение SOM при расчетах будем брать равным 10 дБ.

Потери в свободном пространстве составят:

$$L_{bf} = 20 - 0 + 10 + 0 - 0 - (-61) - 10 = 81 \text{ дБ.}$$

По формуле (Л7.11) находим дальность связи:

$$D = 10^{\left(\frac{81 - 20 \lg(2437) - 32,4}{20} \right)} = 0,110 \text{ км} = 110 \text{ м.}$$

Сделаем расчет для обратного направления линии связи. Передающее устройство — DWA-182, принимающее устройство — DAP-3310.

Потери в свободном пространстве составят:

$$L_{bf} = 15 - 0 + 0 + 10 - 0 - (-69) - 10 = 84 \text{ дБ.}$$

По формуле (7.11) находим дальность связи:

$$D = 10^{\left(\frac{84 - 20 \lg(2437) - 32,4}{20} \right)} = 0,156 \text{ км} = 156 \text{ м.}$$

Вывод: максимальное расстояние между устройствами, при котором они будут стабильно работать на скорости 300 Мбит/с, составляет не более 110 метров.

Шаг 2. Найдем расстояние между устройствами при передаче данных на скорости 1 Мбит/с. Передающее устройство — DAP-3310, принимающее устройство — DWA-182.

Потери в свободном пространстве составят:

$$L_{bf} = 20 - 0 + 10 + 0 - 0 - (-87) - 10 = 107 \text{ дБ.}$$

По формуле (7.11) находим дальность связи:

$$D = 10^{\left(\frac{(107 - 20 \lg(2437) - 32,4)}{20} \right)} = 2,2 \text{ км.}$$

Сделаем расчет для обратного направления линии связи. Передающее устройство — DWA-182, принимающее устройство — DAP-3310.

Потери в свободном пространстве составят:

$$L_{bf} = 19 - 0 + 0 + 10 - 0 - (-96) - 10 = 115 \text{ дБ.}$$

По формуле (7.11) находим дальность связи:

$$D = 10^{\left(\frac{(115 - 20 \lg(2437) - 32,4)}{20} \right)} = 5,5 \text{ км.}$$

Вывод: максимальное расстояние между устройствами, при котором они будут стабильно работать на скорости 1 Мбит/с, составляет не более 2,2 км.

ПРИМЕР 3

Вычислите минимальную высоту установки антенн, чтобы 60 % первой зоны Френеля было свободно от препятствий. Расстояние между антеннами равно 2 км. Передача ведется в диапазоне 2,4 ГГц на 6-м канале (2437 МГц).

РЕШЕНИЕ

Шаг 1. Рассчитаем радиус первой зоны Френеля по формуле (Л7.6):

$$R = 17,32 \sqrt{\frac{2}{4 \cdot 2,437}} = 7,84 \text{ м.}$$

Шаг 2. Вычислим минимальную высоту установки антенн при условии, что 60 % первой зоны Френеля свободно от препятствий, по формуле (Л7.10):

$$H_{ant} = 10,4 \sqrt{\frac{2}{4 \cdot 2,437}} + \frac{2^2}{68} = 4,76 \text{ м.}$$

7.2. Задания для самостоятельного выполнения

Примечание. В заданиях, где не указаны модели беспроводных устройств, студентам предлагается выбрать их самостоятельно. Описания и характеристики устройств можно посмотреть на сайте <http://dlink.ru> → *Продукты и решения* → *Беспроводное оборудование*; потерь в антенно-фидерном тракте, т. е. между беспроводными устройствами и их антеннами, нет (0 дБм).

ЗАДАНИЕ 1

Определите потери в свободном пространстве на линии связи между точкой доступа и клиентским устройством стандарта 802.11n, работающими на 7-м канале (центральная частота 2 442 МГц). Расстояние между устройствами 100 м.

ЗАДАНИЕ 2

Определите потери в свободном пространстве на линии связи между точкой доступа стандарта 802.11n и точкой доступа стандарта 802.11ac, работающими на 64-м канале (центральная частота 5 320 МГц). Расстояние между устройствами 200 м.

ЗАДАНИЕ 3

Вычислите радиус первой зоны Френеля. Расстояние между антеннами 15 км. Расстояние от антенны передатчика до самой высшей точки предполагаемого препятствия 7 км. Передача ведется в диапазоне 2,4 ГГц на 6-м канале (центральная частота 2 437 МГц).

ЗАДАНИЕ 4

Вычислите минимальную высоту установки антенн, чтобы 80 % первой зоны Френеля было свободно от препятствий. Расстояние между антеннами равно 4 км. Передача ведется в диапазоне 5 ГГц на 36-м канале (центральная частота 5 180 МГц).

ЗАДАНИЕ 5

Определите максимальное расстояние, на котором линия связи между DAP-2310 и DWA-160 будет стабильно работать в обоих направлениях при скоростях передачи 300 Мбит/с и 1 Мбит/с.

ЗАДАНИЕ 6

Определите максимальное расстояние, на котором линия связи между DAP-2660 и DWA-182 будет стабильно работать в обоих направлениях на максимальной скорости, поддерживаемой беспроводной сетью. Передача ведется в диапазоне 5 ГГц.

ЗАДАНИЕ 7

Оцените возможность работы канала связи длиной 4 км между точкой доступа DAP-3662 и беспроводным клиентом с адаптером DWA-182 на максимальной скорости, поддерживаемой беспроводной сетью. Устройства работают на 60-м канале (центральная частота 5 300 МГц).

Лабораторная работа № 8. Влияние скорости передачи на производительность и дальность действия сети

Скорость передачи данных (*data rate*), которая обычно указывается в характеристиках беспроводных устройств, является максимально возможной теоретической пропускной способностью сети, достигаемой при использовании конкретной технологии. Однако реальная пропускная способность всегда меньше теоретической, что связано с издержками на передачу служебной информации, количеством клиентов, расстоянием, наличием преград, интерференцией и многим другим. Поддержание надежной работы и безопасности беспроводной сети снижает теоретическую скорость передачи данных примерно на 30...50 %.

Не стоит забывать, что беспроводная среда является разделяемой. Передачи происходят в режиме полудуплекса, где только одно устройство в один момент времени может использовать канал. Поэтому чем больше клиентских устройств подключено к каналу, тем больше трафика они создают и тем меньше реальная скорость передачи.

Скорость передачи данных влияет не только на производительность беспроводной сети, но и на расстояние передачи. Чем выше скорость, тем меньше расстояние, на которое может быть передан сигнал. Основная причина сокращения расстояния при увеличении скорости связана с тем, что большая скорость требует большей мощности сигнала на входе приемника. Производители указывают в характеристиках беспроводного оборудования значение чувствительности для конкретной скорости передачи. Именно чувствительность оборудования определяет достижимую дальность связи для каждой конкретной скорости передачи.

Клиент может достичь максимальной скорости передачи в том случае, если он передает точке доступа и принимает от нее сигнал наибольшей мощности при минимальной интерференции и отсутствии препятствий. В случае удаления клиента от точки доступа или наличия каких-то препятствий на пути сигнала точка доступа автоматически снижает скорость передачи. При приближении клиента к точке доступа скорость автоматически повышается, если на пути сигнала нет препятствий и влияние интерференции незначительно. По умолчанию скорости передачи точки доступа и клиентов устанавливаются автоматически благодаря процессу адаптивного выбора скоростей. Также автоматически при изменении скоростей изменяется мощность передатчика.

Цель работы:

- оценить производительность беспроводной сети при разном количестве подключенных клиентов;
- изучить зависимость дальности действия беспроводной сети от скорости передачи.

Оборудование (на 2 рабочих места):

Ноутбук	1 шт.
Рабочая станция	4 шт.

Беспроводной адаптер DWA-160 или DWA-582	3 шт.
Точка доступа DAP-2310	1 шт.
Антенна ANT24-0502	1 шт.
Кабель Ethernet	1 шт.
ПО — утилита командной строки для анализа пропускной способности сети iperf.	
ПО — программа для мониторинга беспроводных сетей inSSIDer Home.	

8.1. Оценка производительности беспроводной сети

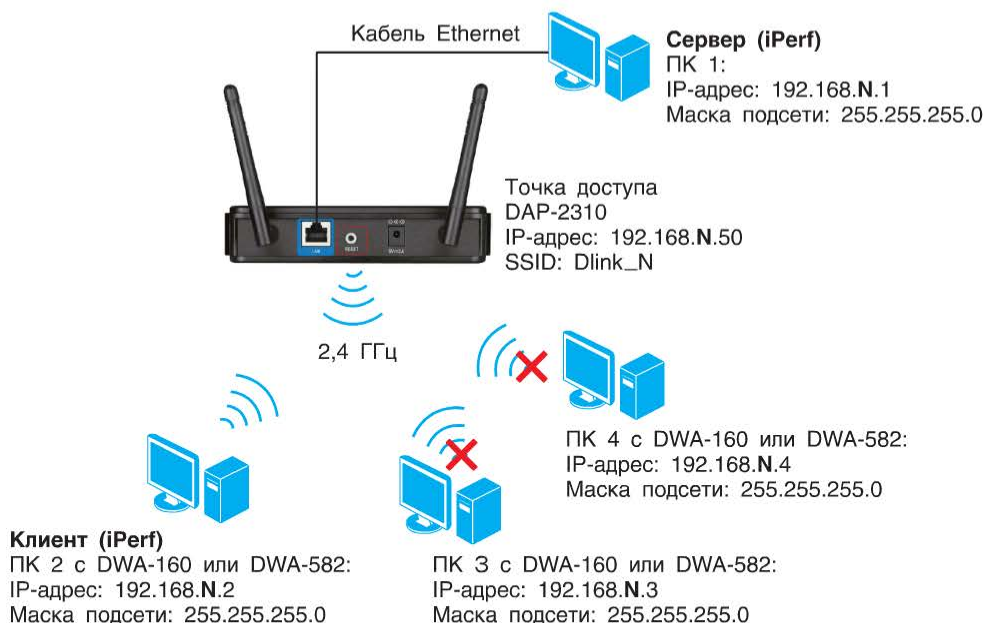


Рис. 8.1. Схема сети для п. 8.1

Перед выполнением задания (рис. 8.1) верните настройки точки доступа к заводским настройкам по умолчанию.

Примечание. Рабочие станции подключаются к беспроводной сети только после особого указания.

Шаг 1. Подключите Ethernet-кабель к LAN-порту точки доступа и к Ethernet-адаптеру рабочей станции ПК1.

Шаг 2. Настройте статический IP-адрес на Ethernet-адаптере рабочей станции ПК 1 — 192.168.0.1 с маской подсети 255.255.255.0.

Шаг 3. Зайдите на Web-интерфейс точки доступа. Измените IP-адрес управления на 192.168.N.50 с маской подсети 255.255.255.0. Сохраните и активируйте настройки.

Шаг 12. Настройте статический IP-адрес на беспроводном интерфейсе ПК 3. Подключитесь к беспроводной сети *Dlink_N*.

Шаг 13. На рабочей станции ПК 3 проверьте доступ к файлу, открытому для общего доступа на рабочей станции ПК 1. Для этого нажмите меню *Пуск* → *Компьютер*. В адресной строке введите `\\192.168.N.1` и нажмите клавишу *Enter*.

Шаг 14. Скопируйте файл с ПК 1 на рабочую станцию ПК 3 одновременно с запуском утилиты iPerf на рабочих станциях ПК 1 и ПК 2.

Средняя скорость передачи данных, выводимая утилитой iPerf _____

Сравните с результатами, полученными на шаге 10 _____

Шаг 15. Настройте статический IP-адрес на беспроводном интерфейсе ПК 4. Подключитесь к беспроводной сети *Dlink_N*.

Шаг 16. На рабочей станции ПК 4 проверьте доступ к файлу, открытому для общего доступа на рабочей станции ПК 1. Для этого нажмите меню *Пуск* → *Компьютер*. В адресной строке введите `\\192.168.N.1` и нажмите клавишу *Enter*.

Шаг 17. На ПК 3 и ПК 4 одновременно запустите копирование файла с ПК 1, а на ПК 1 и ПК 2 синхронно с этим запустите iPerf.

Средняя скорость передачи данных, выводимая утилитой iPerf _____

Сравните с результатами, полученными на шаге 10 и 14 _____

Шаг 18. На рабочей станции ПК 2 проверьте доступ к файлу, открытому для общего доступа на рабочей станции ПК 1. Для этого нажмите меню *Пуск* → *Компьютер*. В адресной строке введите `\\192.168.N.1` и нажмите клавишу *Enter*.

Шаг 19. Одновременно с запуском утилиты iPerf запустите копирование файла на рабочих станциях ПК 2, ПК 3 и ПК 4 с ПК 1.

Средняя скорость передачи данных, выводимая утилитой iPerf _____

Сделайте вывод об изменении производительности сети при увеличении количества одновременно подключенных клиентов _____

Шаг 20. Не возвращайте настройки точки доступа к заводским настройкам по умолчанию.

8.2. Оценка зависимости скорости передачи от дальности действия сети



Рис. 8.4. Схема сети для п. 8.2

Примечание. Для выполнения этого задания потребуется ноутбук с установленной программой inSSIDer и утилитой iPerf.

Шаг 1. Настройте статический IP-адрес на беспроводном интерфейсе ПК 5 и подключитесь к беспроводной сети *Dlink_N*.

Шаг 2. Запустите программу *inSSIDer* на ПК 5. Определите уровень сигнала беспроводной сети *Dlink_N* рядом с точкой доступа. Запишите его _____

Шаг 3. На рабочей станции ПК 1 запустите утилиту iPerf в режиме сервера: `iperf -s -i2`

На ноутбуке ПК 5 запустите утилиту iPerf в режиме клиента: `iperf -c 192.168.N.1 -t240 -i2 -w64k`

Средняя скорость передачи данных, выводимая утилитой iPerf _____

Шаг 4. Отойдите с ПК 5 на такое расстояние от точки доступа, чтобы уровень сигнала беспроводной сети *Dlink_N* уменьшился в 2 раза. Уровень сигнала определите с помощью программы *inSSIDer*. Запишите его _____

Шаг 5. Оцените расстояние (1 шаг = 1 метр), через которое уровень сигнала уменьшился в 2 раза _____

Шаг 6. Средняя скорость передачи данных, выводимая утилитой *iPerf* на данном расстоянии от точки доступа _____

Шаг 7. Подойдите ближе к точке доступа. Средняя скорость передачи данных, выводимая утилитой *iPerf*, увеличивается? _____

Шаг 8. Сделайте вывод о зависимости скорости передачи от дальности действия беспроводной сети _____

8.3. Применение антенны с высоким коэффициентом усиления

Не возвращайте настройки точки доступа к заводским настройкам по умолчанию. Схема сети для данной части лабораторной работы показана на рис. 8.4.

Шаг 1. Запустите программу *inSSIDer* на ПК 5. Определите уровень сигнала беспроводной сети *Dlink_N* рядом с точкой доступа. Запишите его _____

Шаг 2. Отойдите с ПК 5 на расстояние 20 шагов от точки доступа. Запишите уровень сигнала беспроводной сети *Dlink_N*, который отображается в программе *inSSIDer* на данном расстоянии _____

Шаг 3. Замените антенны на точке доступа на ANT24-0502 (рис. 8.5).



Рис. 8.5. Замена антенны на точке доступа DAP-2310

Шаг 4. Отойдите с ПК 5 на расстояние 20 шагов от точки доступа. С помощью программы *inSSIDer* определите уровень сигнала беспроводной сети. Сравните с результатами, полученными на шаге 2. Какой вывод вы можете сделать?

Лабораторная работа № 9. Настройка распределенной сети (WDS)

Механизм WDS является альтернативой традиционному подходу соединения точек доступа через проводную инфраструктуру, но не исключает его. Он позволяет достичь значительной экономии средств, обеспечивает простоту настройки и добавления новых точек доступа в сеть.

При использовании WDS точки доступа могут работать в одном из двух режимов:

- режим беспроводного моста (WDS);
- режим беспроводного моста с функциями точки доступа (WDS with AP).

В режиме WDS точки доступа соединяются только между собой и не позволяют беспроводным клиентам подключаться к ним. В режиме WDS with AP точки доступа не только соединяются между собой, но и обслуживают подключенных беспроводных клиентов.

При работе в обоих режимах точки доступа могут устанавливать мостовые соединения типа «точка—точка» и «точка—много точек». При создании подключений типа «точка—точка» две точки доступа устанавливают между собой мостовое соединение. При этом каждая точка доступа может установить несколько таких соединений с разными точками доступа. Максимальное число соединений зависит от модели точки доступа, обычно их 4 или 8. При создании подключения типа «точка—много точек» точка доступа, используемая как центральная, устанавливает мостовые соединения с множеством точек доступа. Передача данных ведется через центральную точку доступа. При этом периферийные точки доступа друг к другу не подключаются. Максимальное число устройств, с которыми может установить соединение центральная точка доступа, зависит от ее модели (4 или 8 точек доступа).

Благодаря беспроводному соединению точек доступа можно строить беспроводные сети с большой зоной покрытия, а также соединять проводные или беспроводные сегменты, расположенные как на небольшом расстоянии (в соседних зданиях или комнатах), так и на расстояниях до нескольких километров без создания сложной инфраструктуры.

Топологии беспроводных WDS-сетей могут быть разнообразны: линейное подключение, кольцевое подключение, «звезда», ячеистая топология полной и неполной связности.

Цель работы: научиться настраивать WDS-соединения на точках доступа DAP-2310.

Оборудование (на 3 рабочих места):

Рабочая станция	2 шт.
Беспроводной адаптер DWA-160 или DWA-582	2 шт.
Точка доступа DAP-2310	3 шт.
Коммутатор DES-1100-16	2 шт.
Кабель Ethernet	4 шт.

9.1. Настройка WDS-соединения типа «точка—точка»

Перед выполнением задания (рис. 9.1) верните настройки точек доступа и коммутаторов к заводским настройкам по умолчанию.

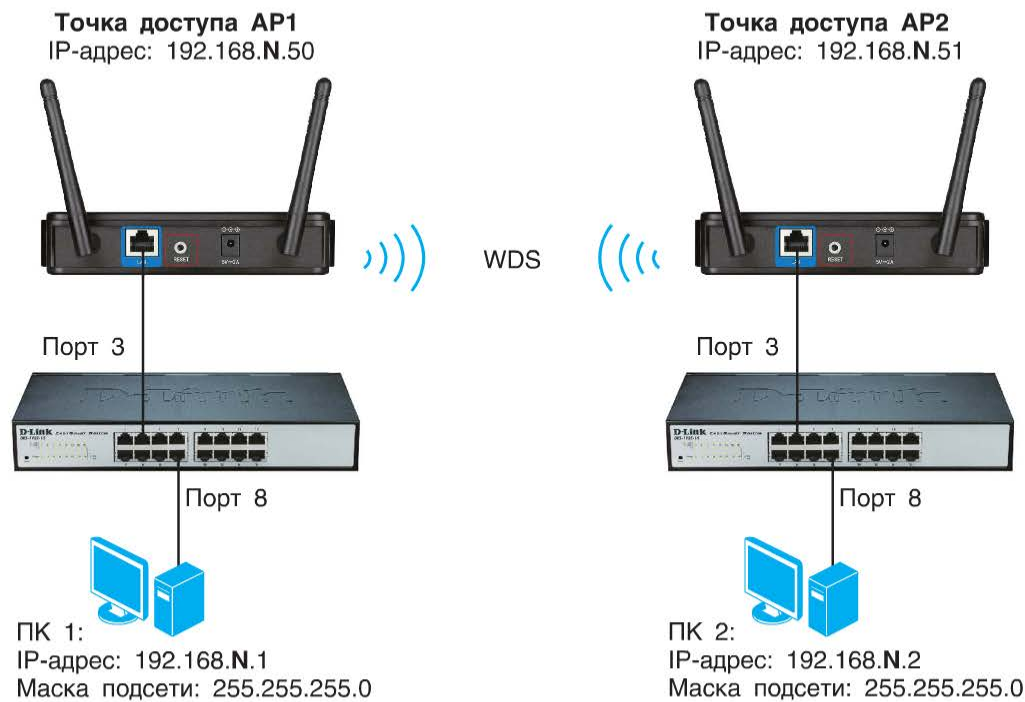


Рис. 9.1. Общая схема сети для п. 9.1

Примечание. Настройка точек доступа выполняется с рабочей станции ПК 1.

Изменение IP-адреса управления точек доступа AP1 и AP2

Шаг 1. Подключите рабочую станцию ПК 1 к LAN-порту точки доступа AP1.

Шаг 2. Настройте статический IP-адрес на Ethernet-адаптере рабочей станции ПК 1 — 192.168.0.1 с маской подсети 255.255.255.0.

Шаг 3. Зайдите на Web-интерфейс точки доступа AP1. Измените IP-адрес управления на 192.168.N.50 с маской подсети 255.255.255.0. Сохраните и активируйте настройки.

Шаг 4. Подключите рабочую станцию ПК 1 к LAN-порту точки доступа AP2.

Шаг 5. Зайдите на Web-интерфейс точки доступа AP2. Измените IP-адрес управления на 192.168.N.51 с маской подсети 255.255.255.0. Сохраните и активируйте настройки.

Шаг 6. Измените IP-адрес Ethernet-адаптера рабочей станции ПК 1 на 192.168.N.1 с маской подсети 255.255.255.0.

Настройка точки доступа AP1 (рис. 9.2)

Шаг 1. Подключите ПК 1 к LAN-порту точки доступа AP1. Зайдите на Web-интерфейс и уменьшите выходную мощность передатчика точки доступа до 12,5 %.

Шаг 2. Выполните настройку WDS-соединения с точкой доступа AP2.

Примечание. Между любой парой точек доступа может быть установлено только одно WDS-соединение. Важно, чтобы настройки WDS-соединения обеих точек доступа были одинаковыми. К этим настройкам относятся: номер канала, ширина канала, SSID, алгоритмы и пароли шифрования. Для этого:

- 1) выберите раздел *Basic Settings* → *Wireless*;
- 2) в списке *Mode* выберите *WDS*;
- 3) в поле *Network Name (SSID)* введите *DlinkWDS_N*;
- 4) в поле *Channel* выберите 6;
- 5) в поле *Channel Width* выберите *20MHz*;
- 6) в окне *Remote AP MAC Address* введите MAC-адрес точки доступа AP2;

Примечание. MAC-адрес указан на наклейке, расположенной на нижней панели точки доступа.

- 7) в выпадающем меню *Authentication* выберите *WPA-Personal*;
- 8) в поле *PassPhrase* введите пароль *DlinkPassword* и повторите его в поле *Confirm PassPhrase*;
- 9) сохраните настройки, нажав кнопку *Save*.

Шаг 3. Сохраните и активируйте настройки. Для этого выберите *Configuration* → *Save and Activate*.

D-Link DAP-2310

Home Maintenance Configuration System Logout Help

DAP-2310

- Basic Settings
 - Wireless
 - LAN
 - IPv6
- Advanced Settings
- Status

Wireless Settings

Wireless Band: 2.4GHz

Mode: WDS

Network Name (SSID): DlinkWDS_0

SSID Visibility: Enable

Auto Channel Selection: Disable

Channel: 6

Channel Width: 20 MHz

WDS

Remote AP MAC Address

1.	2.	3.	4.
fc:75:16:c3:3b:30			
5.	6.	7.	8.

Site Survey

Scan

CH	RSSI	BSSID	Security	SSID
----	------	-------	----------	------

Authentication: WPA-Personal

PassPhrase Settings

WPA Mode: WPA2 Only

Cipher Type: AES

Group Key Update Interval: 3600 (Seconds)

PassPhrase:

Confirm PassPhrase:

notice: 8~63 in ASCII or 64 in Hex
(0-9,a-z,A-Z,~!@#\$\$%^&*0_+~-=\|;':",./<>?)

Save

Рис. 9.2. Настройка точки доступа AP1

Настройка точки доступа AP2

Шаг 1. Подключите ПК 1 к LAN-порту точки доступа AP2. Зайдите на Web-интерфейс и уменьшите выходную мощность передатчика точки доступа до 12,5 %.

Шаг 2. Выполните настройку WDS-соединения с точкой доступа AP1. Для этого:

- 1) выберите раздел *Basic Settings* → *Wireless*;
- 2) в списке *Mode* выберите *WDS*;
- 3) в поле *Network Name (SSID)* введите *DlinkWDS_N*;
- 4) в поле *Channel* выберите 6;
- 5) в поле *Channel Width* выберите *20MHz*;
- 6) в окне *Remote AP MAC Address* введите MAC-адрес точки доступа AP1;
- 7) в выпадающем меню *Authentication* выберите *WPA-Personal*;
- 8) в поле *PassPhrase* введите пароль *DlinkPassword*, повторите его в поле *Confirm PassPhrase*;
- 9) сохраните настройки, нажав кнопку *Save*.

Шаг 3. Сохраните и активируйте настройки.

Шаг 4. Проверьте установление WDS-соединений. Для этого на каждой точке доступа зайдите в раздел *Status* → *WDS Information* (рис. 9.3, 9.4).

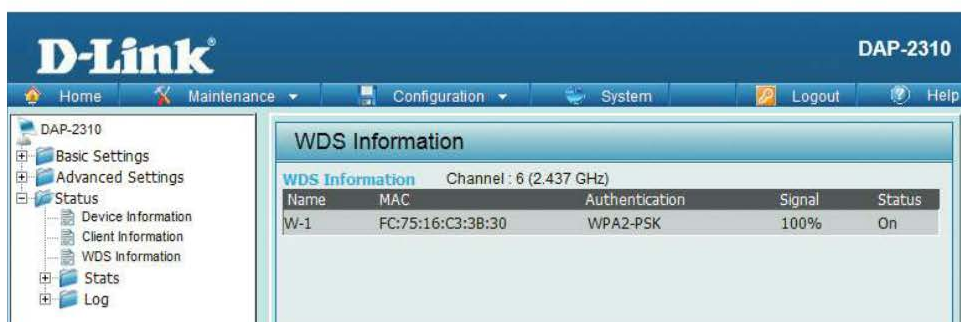


Рис. 9.3. Информация об установленном WDS-соединении на точке доступа AP1



Рис. 9.4. Информация об установленном WDS-соединении на точке доступа AP2

Шаг 5. Подключите устройства, как показано на рис. 9.1. Настройте статический IP-адрес на Ethernet-адаптере ПК 2.

Шаг 6. Проверьте доступность соединения между рабочими станциями командой ping:

от ПК 1 к ПК 2 _____

от ПК 2 к ПК 1 _____

9.2. Настройка WDS-соединения типа «точка—много точек»

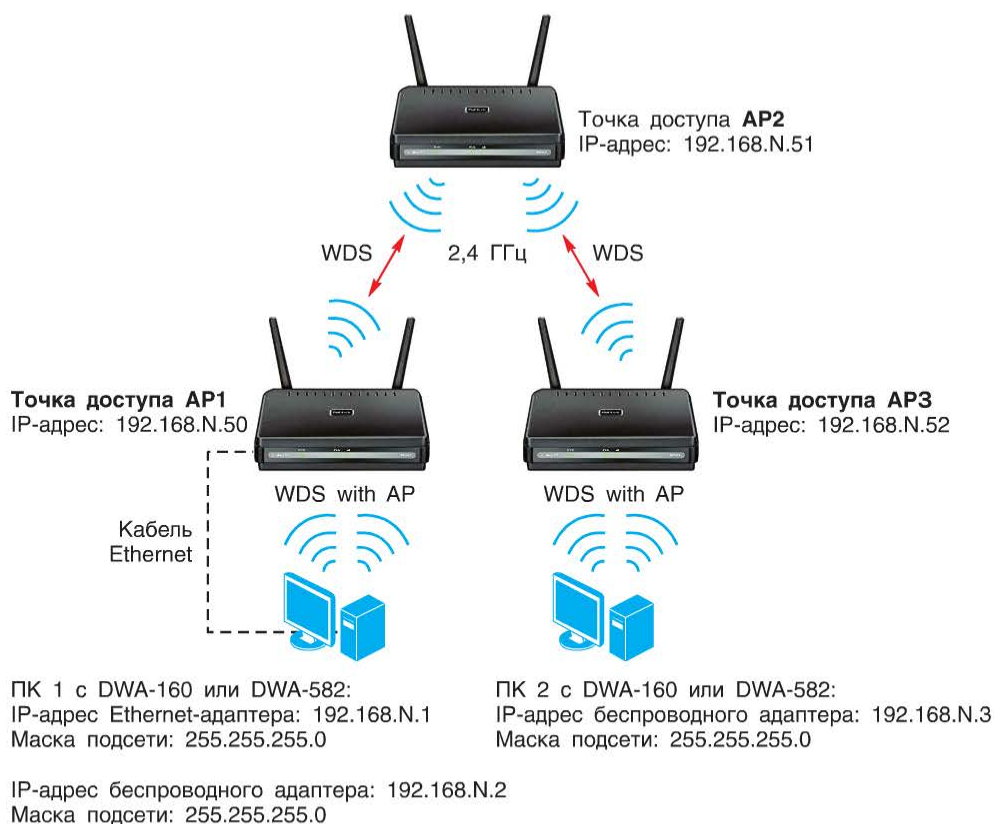


Рис. 9.5. Схема сети для п. 9.2

Перед выполнением задания (рис. 9.5) верните настройки точек доступа к заводским настройкам по умолчанию.

Примечание. Настройка точек доступа выполняется с рабочей станции ПК 1.

Изменение IP-адреса управления точек доступа

Шаг 1. Подключите рабочую станцию ПК 1 к LAN-порту точки доступа AP1.

Шаг 2. Настройте статический IP-адрес на Ethernet-адаптере рабочей станции ПК 1 — 192.168.0.1 с маской подсети 255.255.255.0.

Шаг 3. Зайдите на Web-интерфейс точки доступа AP1. Измените IP-адрес управления на 192.168.N.50 с маской подсети 255.255.255.0. Сохраните и активируйте настройки.

Шаг 4. Подключите рабочую станцию ПК 1 к LAN-порту точки доступа AP2.

Шаг 5. Зайдите на Web-интерфейс точки доступа AP2. Измените IP-адрес управления на 192.168.N.51 с маской подсети 255.255.255.0. Сохраните и активируйте настройки.

Шаг 6. Подключите рабочую станцию ПК 1 к LAN-порту точки доступа AP3.

Шаг 7. Зайдите на Web-интерфейс точки доступа AP3. Измените IP-адрес управления на 192.168.N.52 с маской подсети 255.255.255.0. Сохраните и активируйте настройки.

Шаг 8. Измените IP-адрес Ethernet-адаптера рабочей станции ПК 1 на 192.168.N.1 с маской подсети 255.255.255.0.

Настройка точки доступа AP1 (рис. 9.6)

Шаг 1. Подключите ПК 1 к LAN-порту точки доступа AP1. Зайдите на Web-интерфейс и уменьшите выходную мощность передатчика точки доступа до 12,5 %.

Шаг 2. Настройте режим *WDS with AP*, чтобы точки доступа могли взаимодействовать между собой по типу мостового соединения с возможностью подключения беспроводных клиентов. Для этого:

- 1) выберите раздел *Basic Settings* → *Wireless*;
- 2) в списке *Mode* выберите *WDS with AP*;
- 3) в поле *Network Name (SSID)* введите *Dlink_N*;
- 4) в поле *Channel* выберите 6;
- 5) в поле *Channel Width* выберите *20 MHz*;
- 6) в окне *Remote AP MAC Address* введите MAC-адрес точки доступа AP2;
- 7) в выпадающем меню *Authentication* выберите *WPA-Personal*;
- 8) в поле *PassPhrase* введите пароль *DlinkPassword*, повторите его в поле *Confirm PassPhrase*.

После выполнения всех настроек нажмите кнопку *Save*.

Шаг 3. Для последующей проверки работоспособности создайте ограничивающий список устройств, которые могут ассоциироваться с точкой доступа. Для этого выберите *Advanced Settings* → *Filters* → *Wireless MAC ACL*. Включите фильтрацию подключений к точке доступа по MAC-адресам — в поле *Access Control List* выберите *Accept*. В поле *MAC Address* введите MAC-адрес рабочей станции ПК 1 и нажмите кнопки *Add* и *Save*.

Шаг 4. Сохраните и активируйте настройки.

Рис. 9.6. Настройка точки доступа AP1

Настройка точки доступа AP2

Шаг 1. Подключите ПК 1 к LAN-порту точки доступа AP2. Зайдите на Web-интерфейс и уменьшите выходную мощность передатчика точки доступа до 12,5 %.

Шаг 2. Выполните настройку WDS-соединения с точками доступа AP1 и AP3. Для этого:

- 1) выберите раздел *Basic Settings* → *Wireless*;
- 2) в списке *Mode* выберите *WDS*;
- 3) в поле *Network Name (SSID)* введите *Dlink_N*;
- 4) в поле *Channel* выберите 6;
- 5) в поле *Channel Width* выберите *20 MHz*;
- 6) в окне *Remote AP MAC Address* введите MAC-адреса точек доступа AP1 и AP3;
- 7) в выпадающем меню *Authentication* выберите *WPA-Personal*;
- 8) в поле *PassPhrase* введите пароль *DlinkPassword*, повторите его в поле *Confirm PassPhrase*.

После выполнения всех настроек нажмите кнопку *Save*.

Шаг 3. Сохраните и активируйте настройки.

Настройка точки доступа AP3

Шаг 1. Подключите ПК 1 к LAN-порту точки доступа AP3. Зайдите на Web-интерфейс и уменьшите выходную мощность передатчика точки доступа до 12,5 %.

Шаг 2. Выполните настройку WDS-соединения с точкой доступа AP2.

Шаг 3. Для последующей проверки работоспособности создайте ограничивающий список устройств, которые могут ассоциироваться с точкой доступа. Для этого выберите *Advanced Settings* → *Filters* → *Wireless MAC ACL*. Включите фильтрацию подключений к точке доступа по MAC-адресам — в поле *Access Control List* выберите *Accept*. В поле *MAC Address* введите MAC-адрес рабочей станции ПК 2 и нажмите кнопки *Add* и *Save*.

Шаг 4. Сохраните и активируйте настройки.

Шаг 5. Проверьте установление WDS-соединений. Для этого на каждой точке доступа зайдите в раздел *Status* → *WDS Information*.

Проверка работоспособности схемы

Шаг 1. Настройте статические IP-адреса на беспроводных интерфейсах ПК 1 и ПК 2 в соответствии с рис. 9.5 и номером рабочей группы.

Шаг 2. На ПК 1 и ПК 2 подключитесь к беспроводной сети *Dlink_N*.

Шаг 3. Удостоверьтесь, что ПК 1 и ПК 2 подключились к разным точкам доступа. Для этого на точках доступа AP1 и AP3 зайдите в раздел *Status* → *Client Information*.

Шаг 4. Отключите Ethernet-кабель от ПК 1.

Шаг 5. Проверьте доступность соединения между рабочими станциями командой *ping*:

от ПК 1 к ПК 2 _____
от ПК 2 к ПК 1 _____

Шаг 6. Отключите питание точки доступа AP2.

Шаг 7. Проверьте доступность соединения между рабочими станциями командой ping:

от ПК 1 к ПК 2 _____
от ПК 2 к ПК 1 _____

Шаг 8. Доступно соединение между ПК1 и ПК2? Объясните почему ____

Лабораторная работа № 10. Настройка сегментации сети

Сегментация беспроводной сети позволяет повысить производительность и защищенность сети, а также разграничить доступ к ресурсам. В архитектуре WLAN SSID определяет группу взаимодействующих между собой точек доступа и клиентских устройств. Для того чтобы устройства могли взаимодействовать друг с другом, в их настройках должны быть указаны одинаковые параметры (SSID, настройки безопасности). В беспроводной сети можно определить несколько SSID. Если точка доступа поддерживает функцию Multiple SSID (Multi-SSID), то на базе любого ее физического беспроводного интерфейса может быть создано несколько виртуальных интерфейсов, поддерживающих разные SSID (количество виртуальных интерфейсов зависит от модели точки доступа). Таким образом, различные типы клиентов беспроводной сети (например, гости, сотрудники) или трафик отдельных приложений (например, голос или видео) можно объединить в логические группы на основе разных SSID.

Клиенты, подключенные к беспроводным интерфейсам с разными SSID, могут передавать данные друг другу в пределах одной точки доступа. Для того чтобы трафик разных групп клиентов был полностью изолирован друг от друга, SSID беспроводных интерфейсов (физических и/или виртуальных) привязывают к отдельным виртуальным локальным сетям (VLAN). Таким образом, настройка пары SSID/VLAN позволит разбить беспроводную сеть на сегменты и определить для каждого сегмента свои настройки безопасности, контроля широковещательных сообщений и качества обслуживания (QoS).

Точку доступа можно рассматривать как коммутатор, имеющий следующие порты: управление (Mgmt), локальная сеть (LAN), MSSID и WDS (количество портов MSSID и WDS зависит от модели точки доступа). Любой порт точки доступа может быть настроен как Tag (маркированный), Untag (немаркированный) или Not member. Режим Untag позволяет работать с теми сетевыми устройствами виртуальной сети, которые не понимают тегов в заголовке кадра. Режим Tag позволяет настраивать VLAN между несколь-

кими точками доступа или между точками доступа и коммутаторами, поддерживающими стандарт IEEE 802.1Q. Режим Not member используется для указания портов, которые не включены в VLAN.

Каждый порт точки доступа имеет идентификатор порта VLAN (PVID). Этот параметр используется для того, чтобы определить, в какую VLAN точка доступа направит входящий немаркированный кадр из подключенного к порту сегмента, если кадр нужно передать на другой порт. Точки доступа добавляют в заголовки всех немаркированных кадров беспроводных клиентов идентификатор VID, равный PVID порта MSSID, на который они были приняты. Этот механизм позволяет одновременно существовать в одной сети устройствам с поддержкой и без поддержки стандарта IEEE 802.1Q.

Если на точке доступа не настроены VLAN, то все порты по умолчанию входят в одну VLAN с PVID = 1.

В сетях масштаба предприятия обычно применяются как проводные, так и беспроводные сегменты сети. В этом случае клиенты беспроводной сети могут быть как выделены в отдельную VLAN, так и стать членами соответствующих VLAN проводного сегмента.

Оборудование (на 2 рабочих места):

Рабочая станция	4 шт.
Беспроводной адаптер DWA-160 или DWA-582	4 шт.
Точка доступа DAP-2310	2 шт.
Коммутатор DES-1100-16	1 шт.
Кабель Ethernet	3 шт.

Цель работы: научиться настраивать Multi-SSID и VLAN на точке доступа DAP-2310.

10.1. Настройка сегментации проводной и беспроводной сети

Перед выполнением задания (рис. 10.1) верните настройки точки доступа и коммутатора к заводским настройкам по умолчанию.

Примечание. Настройки точки доступа и коммутатора выполняются с рабочей станции ПК 1.

Настройка точки доступа

Шаг 1. Подключите рабочую станцию ПК 1 к LAN-порту точки доступа.

Шаг 2. Настройте статический IP-адрес на Ethernet-адаптере рабочей станции ПК 1 — 192.168.0.1 с маской подсети 255.255.255.0.

Шаг 3. Зайдите на Web-интерфейс точки доступа. Измените IP-адрес управления на 192.168.N.50 с маской подсети 255.255.255.0. Сохраните и активируйте настройки.

Шаг 4. Измените IP-адрес Ethernet-адаптера рабочей станции ПК 1 на 192.168.N.1 с маской подсети 255.255.255.0.

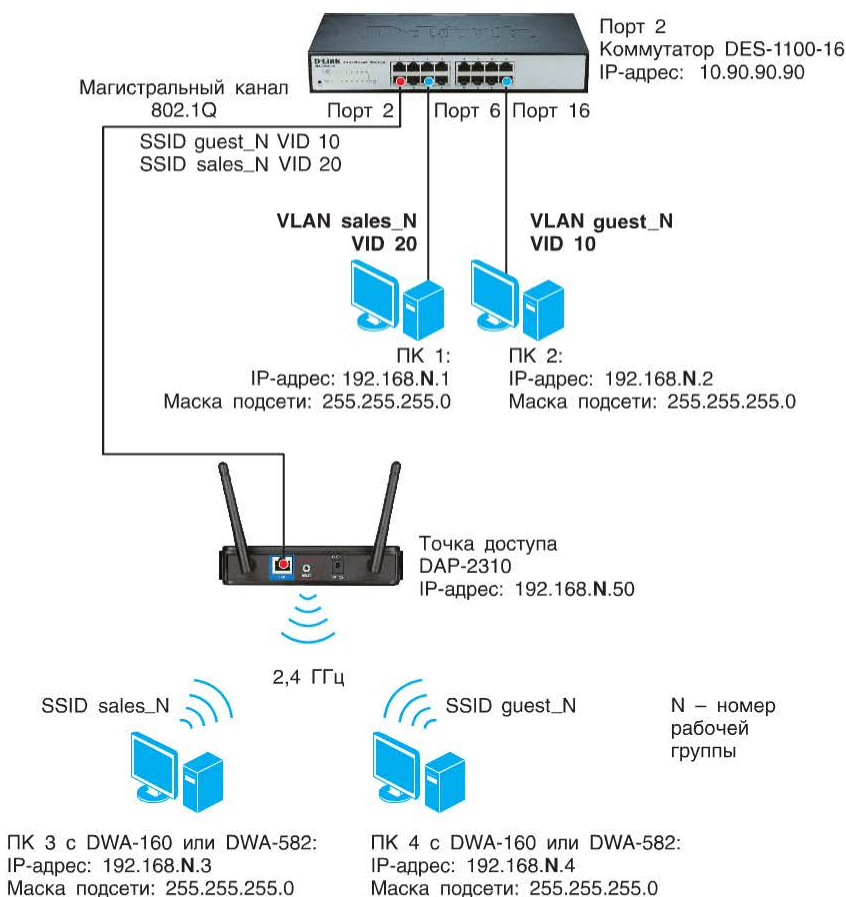


Рис. 10.1. Общая схема сети для п. 10.1

Шаг 5. Повторно зайдите на Web-интерфейс точки доступа и уменьшите выходную мощность передатчика точки доступа до 12,5 %.

Примечание. Программное обеспечение точки доступа DAP-2310 разрешает создавать до семи дополнительных SSID, что позволяет разбить беспроводную сеть на несколько сегментов. Каждый беспроводной сегмент, ассоциированный с соответствующим SSID, может иметь различные настройки параметров шифрования.

Шаг 6. Включите поддержку функции Multi-SSID и создайте два сегмента беспроводной сети с SSID *guest_N* и *sales_N* (рис. 10.2). Для этого:

- 1) выберите *Advanced Settings* → *Multi-SSID*;
- 2) активируйте функцию *Multi-SSID*, поставив галочку в *Enable Multi-SSID*;
- 3) в выпадающем списке *Index* выберите *SSID1*;
- 4) в поле *SSID* введите *guest_N*;
- 5) в выпадающем меню *Security* выберите *WPA-Personal*;

4) в поле *PassPhrase* введите пароль *DlinkQwerty* и повторите его в поле *Confirm PassPhrase*;

5) нажмите кнопку *Add*.

Сохраните созданные SSID, нажав кнопку *Save* (рис. 10.3).

Шаг 7. Настройте привязки SSID и VLAN. Трафик беспроводной сети с *SSID guest_N* должен направляться в *VLAN guest_N* (VID 10), а беспроводной сети с *SSID sales_N* — в *VLAN sales_N* (VID 20). Порты MSSID 1 (*S-1*) и MSSID 2 (*S-2*) являются немаркированными портами VLAN *guest_N* и VLAN *sales_N* соответственно. LAN-порт (LAN) является маркированным портом VLAN *guest_N* и VLAN *sales_N*. Для этого:

1) зайдите во вкладку *Advanced Settings* → *VLAN* и включите поддержку VLAN, выбрав *Enable* в поле *VLAN Status*. Нажмите кнопку *Save* (рис. 10.4);

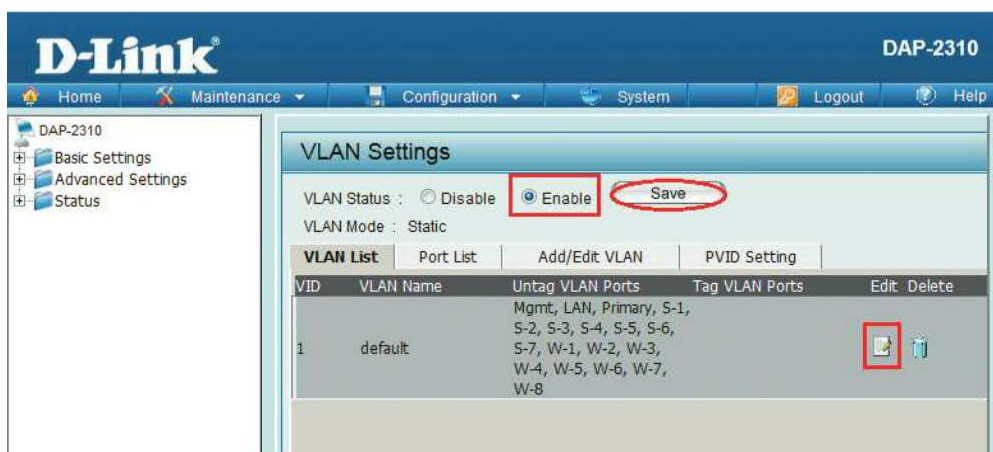


Рис. 10.4. Редактирование VLAN по умолчанию

2) удалите порты из VLAN по умолчанию (default). Во вкладке *VLAN List* нажмите *Edit*;

3) в открывшемся окне установите галочки *Not Member* для портов *S-1* и *S-2*, нажмите кнопку *Save* (рис. 10.5);

4) выберите вкладку *Add/Edit VLAN*, в поле *VLAN ID (VID)* введите *10*, в поле *VLAN Name* — *guest_N*. LAN-порт включите в VLAN как маркированный, MSSID-порт *S-1* как немаркированный. Остальные MSSID и WDS-порты отметьте как *Not Member*. Нажмите кнопку *Save* (рис. 10.6).

Аналогичным образом создайте *VLAN sales_N* с VID 20. Настройте *LAN-port* как маркированный, MSSID-порт *S-2* как немаркированный. Остальные MSSID и WDS-порты отметьте как *Not Member*.

Шаг 8. Просмотрите созданные VLAN. Зайдите во вкладку *Advanced Settings* → *VLAN* → *VLAN List* (рис. 10.7).

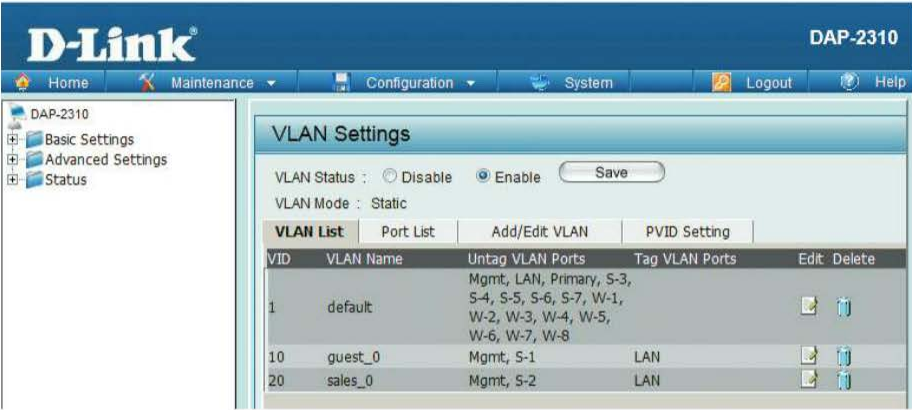


Рис. 10.7. Созданные VLAN

Шаг 9. Назначьте PVID немаркированным MSSID-портам *S-1* и *S-2*. Для этого выберите вкладку *PVID Setting*. В поле *S-1* введите *10*, в поле *S-2* – *20*. Нажмите кнопку *Save* (рис. 10.8).

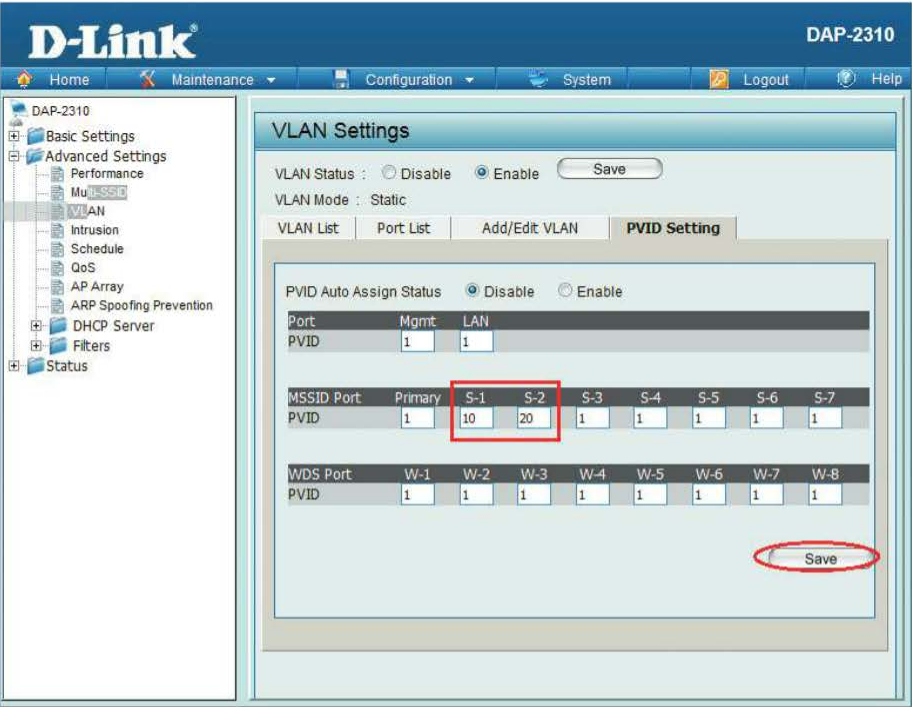


Рис. 10.8. Настройка PVID для MSSID-портов S-1 и S-2

Шаг 10. Сохраните и активируйте настройки.

Настройка VLAN на коммутаторе с поддержкой IEEE 802.1Q

Внимание: при настройке на коммутаторе VLAN на основе стандарта IEEE 802.1Q через Web-интерфейс необходимо, чтобы рабочая станция, с которой осуществляется управление коммутатором, была подключена к порту, входящему в VLAN по умолчанию (default VLAN с VID = 1).

Шаг 1. Подключите рабочую станцию ПК 1 к порту 1 коммутатора.

Шаг 2. На рабочей станции ПК 1 измените статический IP-адрес на 10.90.90.92 с маской подсети 255.0.0.0.

Шаг 3. Зайдите на Web-интерфейс коммутатора. Для этого запустите Web-браузер (Internet Explorer, Mozilla Firefox), в адресной строке которого укажите IP-адрес интерфейса управления коммутатора по умолчанию: `http://10.90.90.90`. В появившемся окне аутентификации, в поле *Password* введите *admin* и нажмите кнопку *Ok*.

Примечание. IP-адрес управления коммутатора по умолчанию обычно указывается в руководстве пользователя. Для коммутатора D-Link DES-1100-16 IP-адрес управления по умолчанию — 10.90.90.90

Шаг 4. Включите функцию 802.1Q глобально на коммутаторе. Для этого выберите раздел *VLAN* → *802.1Q VLAN* и установите галочку *802.1Q VLAN* → *Enabled*. Нажмите кнопку *Apply* (рис. 10.9).

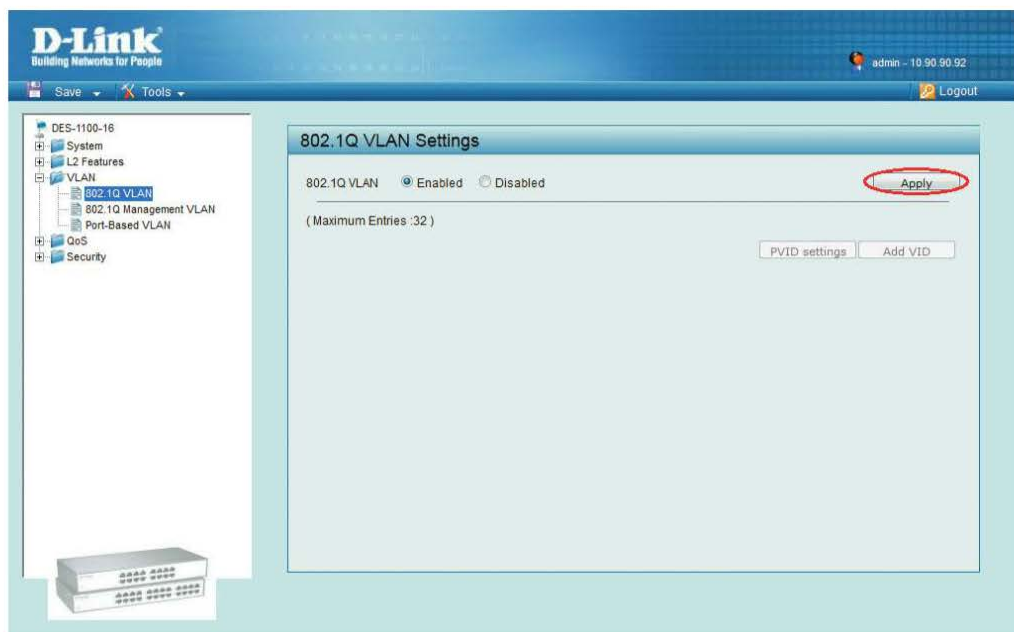


Рис. 10.9. Включение функции 802.1Q глобально на коммутаторе

Шаг 5. Удалите порты из VLAN по умолчанию (default VLAN). Выберите раздел *VLAN* → *802.1Q VLAN* и нажмите ссылку *VID 1* (рис. 10.10).

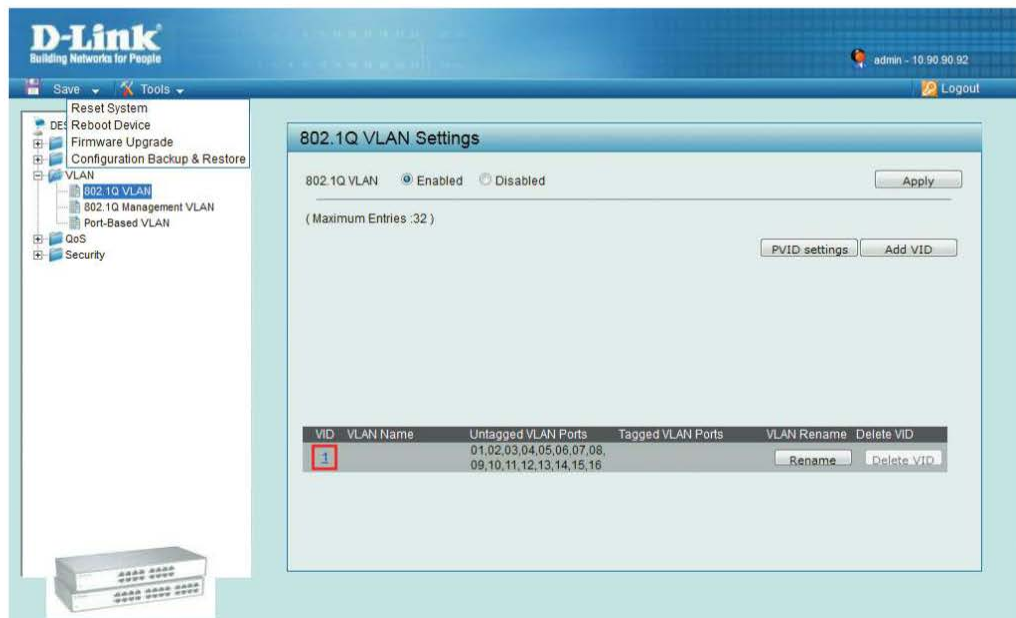


Рис. 10.10. Редактирование VLAN по умолчанию

Примечание. В заводских установках по умолчанию все порты коммутатора назначены в default VLAN с VID = 1. Перед созданием новой VLAN необходимо удалить из default VLAN все порты, которые требуется сделать немаркированными членами новой VLAN. Немаркированные порты не могут одновременно быть членами нескольких VLAN.

В открывшемся окне напротив *Not Member* установите галочки для портов 5–8 и 13–16. Нажмите кнопку *Apply* (рис. 10.11).

Шаг 6. Создайте VLAN с именем *sales_N* и настройте порты 5–8 как немаркированные, порт 2 как маркированный. Для этого нажмите кнопку *Add VID* (рис. 10.12).

В поле *VID* введите *20*, в поле *VLAN Name* — *sales_N*, установите галочки напротив *Untagged* для портов 5–8, напротив *Tagged* — для порта 2. Нажмите кнопку *Apply* (рис. 10.13).

Шаг 7. Создайте VLAN с именем *guest_N* и VID *10*, добавьте порты 13–16 в VLAN как немаркированные, порт 2 как маркированный.

Шаг 8. Посмотрите созданные VLAN на коммутаторе. Выберите *VLAN* → *802.1Q VLAN* (рис. 10.14).

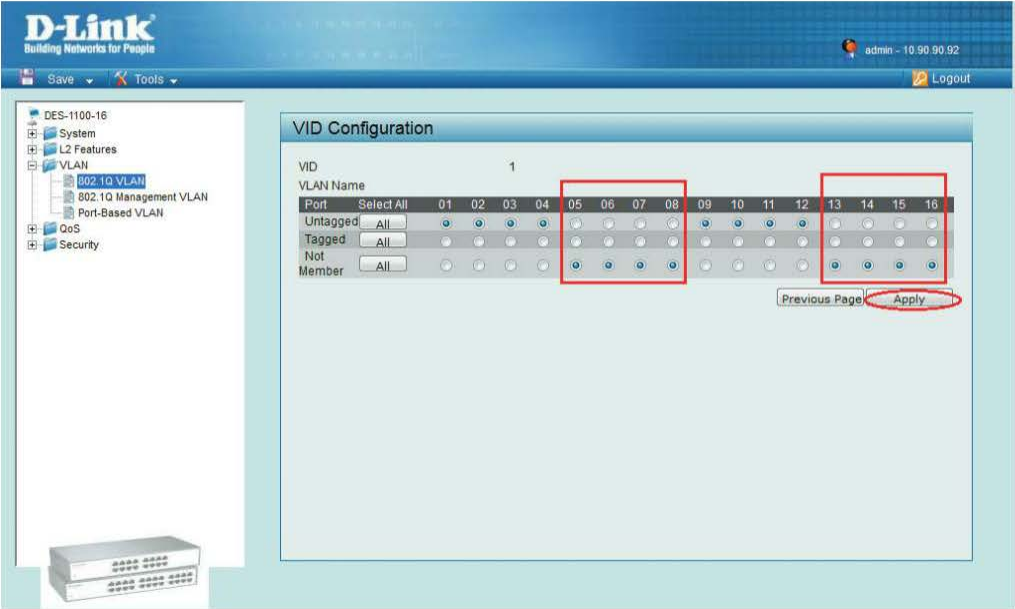


Рис. 10.11. Удаление портов из VLAN по умолчанию

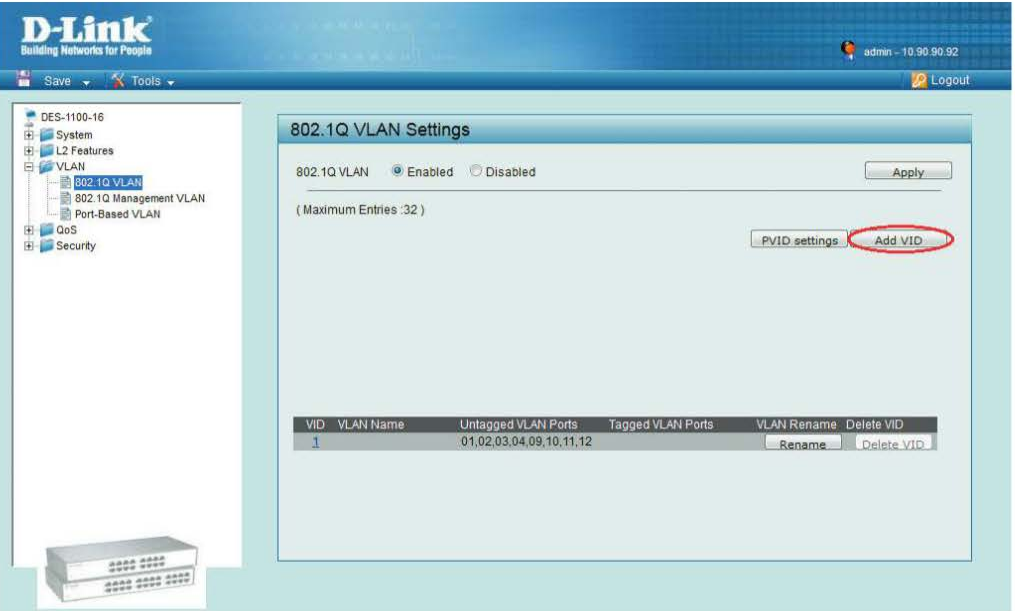


Рис. 10.12. Создание VLAN sales_0

Проверка работоспособности схемы

Шаг 1. Настройте на беспроводных интерфейсах ПК 3 и ПК 4 статические IP-адреса в соответствии с рис. 10.1 и номером рабочей группы.

Шаг 2. Настройте на адаптерах Ethernet ПК 1 и ПК 2 статические IP-адреса в соответствии с рис. 10.1 и номером рабочей группы.

Шаг 3. Рабочую станцию ПК 1 подключите к порту 6 коммутатора, а рабочую станцию ПК 2 — к порту 16.

Шаг 4. Рабочую станцию ПК 3 подключите к беспроводной сети *sales_N*, а рабочую станцию ПК 4 — к беспроводной сети *guest_N*.

Шаг 5. Проверьте доступность соединения между рабочими станциями командой *ping*:

от ПК 1 к ПК 3 _____

от ПК 2 к ПК 4 _____

от ПК 1 к ПК 4 _____

от ПК 2 к ПК 3 _____

от ПК 1 к ПК 2 _____

от ПК 3 к ПК 4 _____

Объясните наличие/отсутствие связи между рабочими станциями _____

10.2. Настройка сегментации распределенной сети

Перед выполнением задания (рис. 10.15) верните настройки точек доступа к заводским настройкам по умолчанию.

Примечание. Настройка точек доступа выполняется с рабочей станции ПК 1.

Изменение IP-адреса управления точек доступа AP1 и AP2

Шаг 1. Подключите рабочую станцию ПК 1 к LAN-порту точки доступа AP1.

Шаг 2. Настройте статический IP-адрес на Ethernet-адаптере рабочей станции ПК 1 — 192.168.0.1 с маской подсети 255.255.255.0.

Шаг 3. Зайдите на Web-интерфейс точки доступа AP1. Измените IP-адрес управления на 192.168.N.50 с маской подсети 255.255.255.0. Сохраните и активируйте настройки.

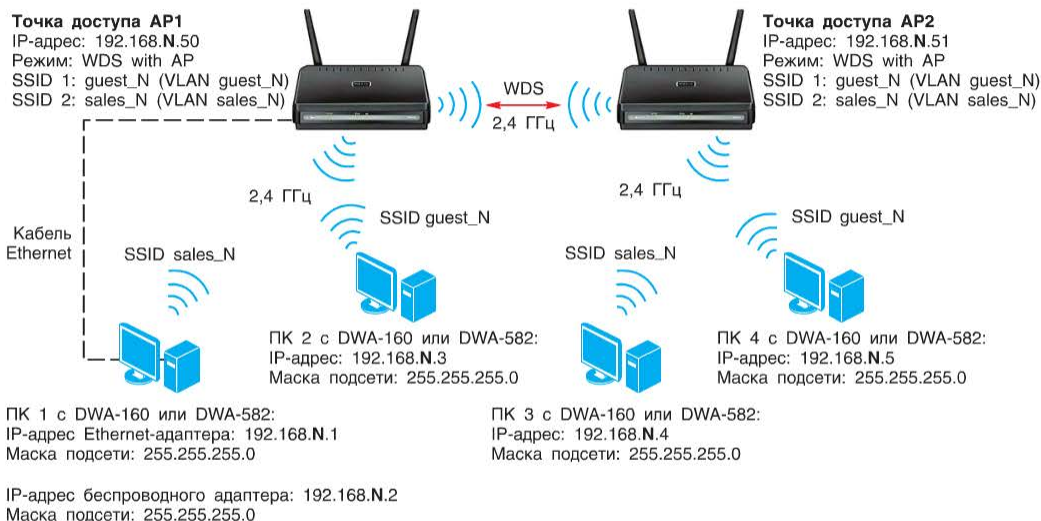


Рис. 10.15. Общая схема сети для п. 10.2

Шаг 4. Подключите рабочую станцию ПК 1 к LAN-порту точки доступа AP2.

Шаг 5. Зайдите на Web-интерфейс точки доступа AP2. Измените IP-адрес управления на 192.168.N.51 с маской подсети 255.255.255.0. Сохраните и активируйте настройки.

Шаг 6. Измените IP-адрес Ethernet-адаптера рабочей станции ПК 1 на 192.168.N.1 с маской подсети 255.255.255.0.

Настройка точки доступа AP1

Шаг 1. Подключите ПК 1 к LAN-порту точки доступа AP1. Зайдите на Web-интерфейс и уменьшите выходную мощность передатчика точки доступа до 12,5 %.

Шаг 2. Настройте режим *WDS with AP*, чтобы точки доступа могли взаимодействовать между собой по типу мостового соединения с возможностью подключения беспроводных клиентов. Для этого:

- 1) выберите вкладку *Basic Settings* → *Wireless*;
- 2) в поле *Mode* выберите *WDS with AP*;
- 3) в поле *Network Name (SSID)* введите *DlinkWDS_N*;
- 4) в поле *Channel* выберите *11*;
- 5) в окне *Remote AP MAC Address* введите MAC-адрес точки доступа AP2;
- 6) в выпадающем меню *Authentication* выберите *WPA-Personal*;
- 7) в поле *PassPhrase* введите пароль *DlinkPassword*, повторите его в поле *Confirm PassPhrase*;
- 8) сохраните настройки, нажав кнопку *Save*.

Шаг 3. Включите поддержку функции Multi-SSID и создайте два сегмента беспроводной сети с SSID *guest_N* и *sales_N*. Для этого:

- 1) зайдите во вкладку *Advanced Settings* → *Multi-SSID*;
- 2) активируйте функцию *Multi-SSID*, поставив галочку в *Enable Multi-SSID*;
- 3) в выпадающем списке *Index* выберите *SSID1*;
- 4) в поле *SSID* введите *guest_N*;
- 5) в выпадающем меню *Security* выберите *WPA-Personal*;
- 6) в поле *PassPhrase* введите *PasswordDlink* и повторите его в поле *Confirm PassPhrase*;
- 7) нажмите кнопку *Add* (рис. 10.16).

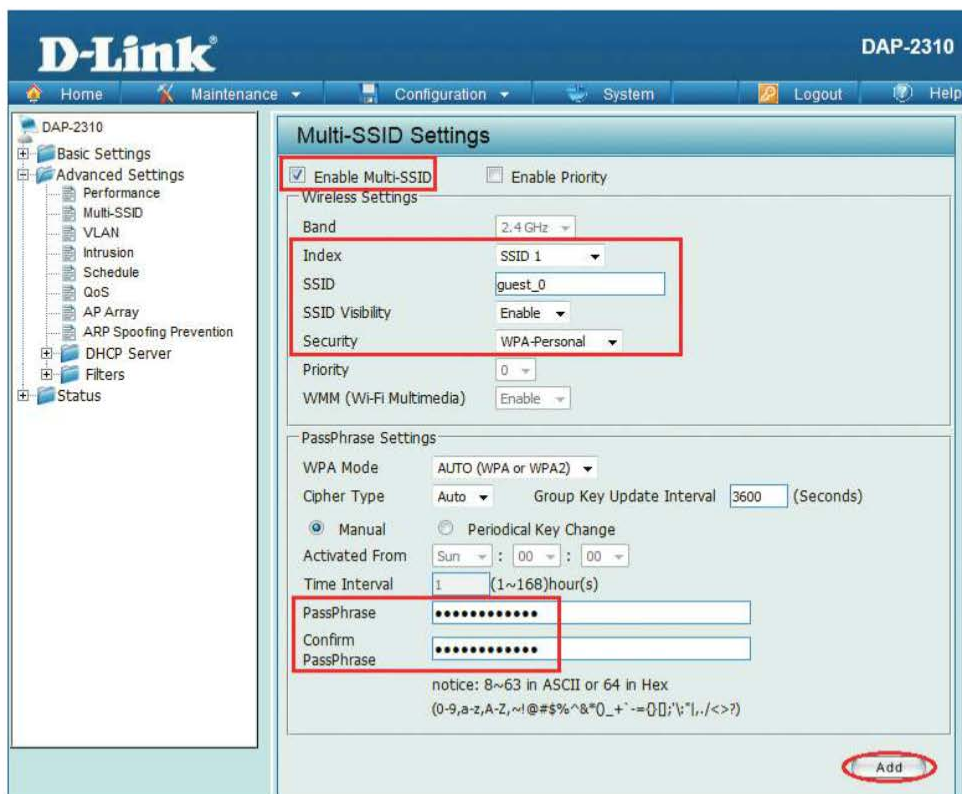


Рис. 10.16. Создание сегмента сети с SSID *guest_0*

Аналогичным образом создайте *SSID2 sales_N*. Для этого:

- 1) в выпадающем списке *Index* выберите *SSID2*;
- 2) в поле *SSID* введите *sales_N*;
- 3) в выпадающем меню *Security* выберите *WPA-Personal*;
- 4) в поле *PassPhrase* введите *DlinkQwerty* и повторите его в поле *Confirm PassPhrase*;

- 5) нажмите кнопку *Add*;
- 6) сохраните созданные Multi-SSID, нажав кнопку *Save* (рис. 10.17).

Index	SSID	Band	Encryption	Delete
Primary SSID	DlinkWDS_0	2.4 GHz	WPA2-Auto-Personal	
Multi-SSID1	guest_0	2.4 GHz	WPA2-Auto-Personal	
Multi-SSID2	sales_0	2.4 GHz	WPA2-Auto-Personal	

Save

Рис. 10.17. Созданные сегменты с SSID guest_0 и SSID sales_0

Шаг 4. Настройте привязку SSID и VLAN. Трафик беспроводной сети с *SSID guest_N* должен направляться в *VLAN guest_N* (VID 10), а беспроводной сети с *SSID sales_N* — в *VLAN sales_N* (VID 20). Порты MSSID 1 (*S-I*) и MSSID 2 (*S-2*)

D-Link®DAP-2310

HomeMaintenanceConfigurationSystemLogoutHelp

DAP-2310

- Basic Settings
- Advanced Settings
- Status

VLAN Settings

VLAN Status : ☐ Disable ☒ Enable Save

VLAN Mode : Static

VLAN ListPort ListAdd/Edit VLANPVID Setting

VLAN ID (VID)10VLAN Nameguest_0

Port	Select All	Mgmt	LAN
Untag	All	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Tag	All	<input type="radio"/>	<input type="radio"/>
Not Member	All	<input type="radio"/>	<input type="radio"/>

MSSID Port	Select All	Primary	S-1	S-2	S-3	S-4	S-5	S-6	S-7
Untag	All	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Tag	All	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Not Member	All	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

WDS Port	Select All	W-1	W-2	W-3	W-4	W-5	W-6	W-7	W-8
Untag	All	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Tag	All	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Not Member	All	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Save

Рис. 10.18. Создание VLAN guest_0

обеих точек доступа являются немаркированными портами VLAN guest_N и VLAN sales_N соответственно. Порт WDS (W-1) обеих точек доступа является маркированным портом VLAN guest_N и VLAN sales_N. Для этого:

1) зайдите во вкладку *Advanced Settings* → *VLAN* и включите поддержку VLAN, выбрав *Enable* в поле *VLAN Status*. Нажмите кнопку *Save*;

2) удалите порты из VLAN по умолчанию (default). Во вкладке *VLAN List* нажмите *Edit*;

3) в открывшемся окне установите галочки *Not Member* для портов *S-1*, *S-2* и *W-1*. Нажмите кнопку *Save*;

4) выберите вкладку *Add/Edit VLAN*. В поле *VLAN ID (VID)* введите *10*, в поле *VLAN Name* — *guest_N*. WDS-порт *W-1* включите в VLAN как маркированный, MSSID-порт *S-1* — как немаркированный. Остальные MSSID и WDS-порты отметьте как *Not Member*. Нажмите кнопку *Save* (рис. 10.18).

Аналогичным образом создайте *VLAN sales_N* с *VID 20*. Настройте WDS-порт *W-1* как маркированный, MSSID-порт *S-2* как немаркированный. Остальные MSSID и WDS-порты отметьте как *Not Member*.

Шаг 5. Просмотрите созданные VLAN. Для этого зайдите во вкладку *Advanced Settings* → *VLAN* → *VLAN List*.

Шаг 6. Назначьте PVID немаркированным MSSID-портам *S-1* и *S-2*. Для этого выберите вкладку *PVID Setting*. В поле *S-1* введите *10*, в поле *S-2* — *20*. Нажмите кнопку *Save*.

Примечание. Использование Multi-SSID без привязки SSID и VLAN позволит беспроводным клиентам, подключенным к разным SSID на одной точке доступа, взаимодействовать между собой. Это может привести к нарушению безопасности беспроводной сети.

Шаг 7. Для последующей проверки работоспособности установите ограничение на устройства, которые могут ассоциироваться с точкой доступа. Для этого выберите *Advanced Settings* → *Filters* → *Wireless MAC ACL*. Включите фильтрацию подключений к точке доступа по MAC-адресам — в поле *Access Control List* выберите *Accept*. В поле *MAC Address* введите MAC-адрес рабочей станции ПК 1 и нажмите кнопку *Add*; далее в поле *MAC Address* введите MAC-адрес рабочей станции ПК 2 и нажмите кнопки *Add* и *Save*.

Шаг 8. Сохраните и активируйте настройки. Выберите *Configuration* → *Save and Activate*.

Настройка точки доступа AP2

Шаг 1–6. Выполните настройку точки доступа AP2 аналогично настройке точки доступа AP1 (шаги 1–6).

Примечание. При настройке режима WDS with AP укажите MAC-адрес точки доступа AP1.

Шаг 7. Для последующей проверки работоспособности установите ограничение на устройства, которые могут ассоциироваться с точкой доступа.

Для этого выберите *Advanced Settings* → *Filters* → *Wireless MAC ACL*. Включите фильтрацию подключений к точке доступа по MAC-адресам — в поле *Access Control List* выберите *Accept*. В поле *MAC Address* введите MAC-адрес рабочей станции ПК 3 и нажмите кнопку *Add*; далее в поле *MAC Address* введите MAC-адрес рабочей станции ПК 4 и нажмите кнопки *Add* и *Save*.

Шаг 8. Удостоверьтесь, что WDS-соединение установлено. Проверьте на точках доступа AP1 и AP2 информацию во вкладке *Status* → *WDS Information*.

Проверка работоспособности схемы

Шаг 1. Настройте статические IP-адреса на беспроводных интерфейсах ПК 1, ПК 2, ПК 3 и ПК 4 в соответствии рис. 10.15 и номером рабочей группы.

Шаг 2. Рабочие станции ПК 1 и ПК 3 подключите к беспроводной сети *sales_N*, рабочие станции ПК 2 и ПК 4 — к беспроводной сети *guest_N*.

Шаг 3. Удостоверьтесь, что ПК 1 и ПК 2 подключились к точке доступа AP1, ПК 3 и ПК 4 — к точке доступа AP2. Для этого на точках доступа зайдите в раздел *Status* → *Client Information*.

Шаг 4. Отключите кабель Ethernet от ПК 1.

Шаг 5. Проверьте доступность соединения между рабочими станциями командой *ping*:

- от ПК 1 к ПК 3 _____
- от ПК 2 к ПК 4 _____
- от ПК 1 к ПК 4 _____
- от ПК 2 к ПК 3 _____
- от ПК 1 к ПК 2 _____
- от ПК 3 к ПК 4 _____

Объясните наличие/отсутствие связи между рабочими станциями _____

Лабораторная работа № 11. Настройка функции AP Array

AP Array является средством централизованного управления группой автономных точек доступа, соединенных друг с другом через проводную сеть Ethernet. Эта функция встроена в программное обеспечение устройств и доступна для настройки через Web-интерфейс.

При использовании AP Array администратору требуется вручную настроить только одну точку доступа. Далее созданная конфигурация автоматически применяется к остальным точкам доступа, входящим в группу. В группу AP

Array может быть объединено до 32 точек доступа D-Link серии DAP-xxx, поддерживающих функцию AP Array 2.0 (предыдущая версия функции позволяла объединять в группу до восьми устройств). Количество самих групп не ограничено, но требуется, чтобы все группы в пределах одной IP-подсети имели разные имена. В группу могут быть объединены точки доступа разных моделей при условии, что они поддерживают функцию AP Array одинаковой версии.

Для того чтобы точка доступа могла вступить в группу AP Array, в ее настройках необходимо указать имя группы и пароль. Каждая точка доступа может быть членом только одной группы AP Array. Следует отметить, что в группу AP Array можно объединять только точки доступа, принадлежащие одной IP-подсети.

Существует три роли, которые точка доступа может выполнять в группе AP Array:

- ведущая точка доступа (Master) управляет настройками всех членов группы. В каждой группе может быть только одна ведущая точка доступа;
- резервная ведущая точка доступа (Backup Master) берет на себя функции ведущей точки доступа, если та выходит из строя. Каждая группа может иметь несколько резервных ведущих точек доступа;
- ведомая точка доступа (Slave) автоматически получает настройки от ведущей точки доступа.

При включении в группу несколько ведущих точек доступа точка доступа, работающая в сети дольше всех, станет ведущей (Master), а включенные позже — резервными (Backup Master).

Ведущая точка доступа синхронизирует настройки со всеми ведомыми и резервными точками доступа всякий раз, когда в ее конфигурацию вносятся изменения и нажимают в Web-интерфейсе кнопку «Save & Activate». При этом существует возможность выбора параметров, настройки которых будут применяться к резервным и ведомым точкам доступа. Остальные параметры при необходимости должны быть индивидуально настроены на каждой точке доступа, входящей в группу AP Array.

Ведущая точка доступа с интервалом одна минута отправляет сигнал проверки статуса ведомых точек доступа. Если какие-либо из них были сконфигурированы вручную, ведущая точка доступа автоматически синхронизирует их конфигурацию.

При выходе ведущей точки доступа из строя ее роль берет на себя резервная точка доступа. В том случае, если резервная точка доступа не была настроена и при этом в сети остались только ведомые точки доступа, они будут функционировать как обычные автономные точки доступа до тех пор, пока в сети снова не появится ведущая точка доступа.

При объединении точек доступа в группу AP Array можно не только централизованно управлять ими, но и выполнять балансировку нагрузки между ними на основе использования полосы пропускания.

Оборудование (на 3 рабочих места):

Рабочая станция	1 шт.
Точка доступа DAP-2310	3 шт.
Коммутатор DES-1100-16	1 шт.
Кабель Ethernet	4 шт.

Цель работы: научиться настраивать функцию AP Аггау на точках доступа DAP-2310.

Перед выполнением задания верните настройки точек доступа и коммутатора к заводским настройкам по умолчанию. Подключите точку доступа AP1 и ПК 1 к портам коммутатора, как показано на рис. 11.1.

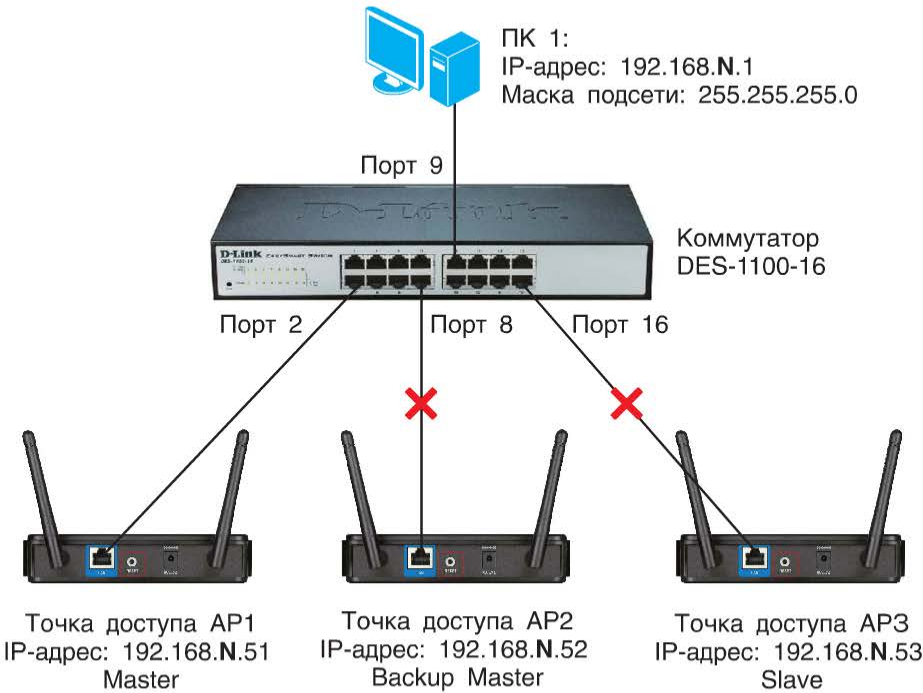


Рис. 11.1. Общая схема сети

Изменение IP-адреса управления точек доступа AP1, AP2 и AP3

Шаг 1. Настройте статический IP-адрес на Ethernet-адаптере рабочей станции ПК 1 — 192.168.0.1 с маской подсети 255.255.255.0.

Шаг 2. Зайдите на Web-интерфейс точки доступа AP1. Измените IP-адрес управления на 192.168.N.51 с маской подсети 255.255.255.0. Сохраните и активируйте настройки.

Шаг 3. Зайдите на Web-интерфейс точки доступа AP2. Измените IP-адрес управления на 192.168.N.52 с маской подсети 255.255.255.0. Сохраните и активируйте настройки.

Шаг 4. Зайдите на Web-интерфейс точки доступа AP3. Измените IP-адрес управления на 192.168.N.53 с маской подсети 255.255.255.0. Сохраните и активируйте настройки.

Шаг 5. Измените IP-адрес Ethernet-адаптера рабочей станции ПК 1 на 192.168.N.1 с маской подсети 255.255.255.0.

Настройка точки доступа AP1

Шаг 1. Повторно зайдите на Web-интерфейс точки доступа AP1 и уменьшите выходную мощность передатчика точки доступа до 12,5 %.

Шаг 2. Настройте точку доступа AP1 ведущей (master) в группе AP Array. Для этого выберите *Advanced Settings* → *AP Array*, установите галочку *Enable AP Array* и переключатель *Master*, в поле *AP Array Name* введите *classroom*, в поле *AP Array Password* введите *DlinkPassword*. Нажмите кнопку *Save* (рис. 11.2).

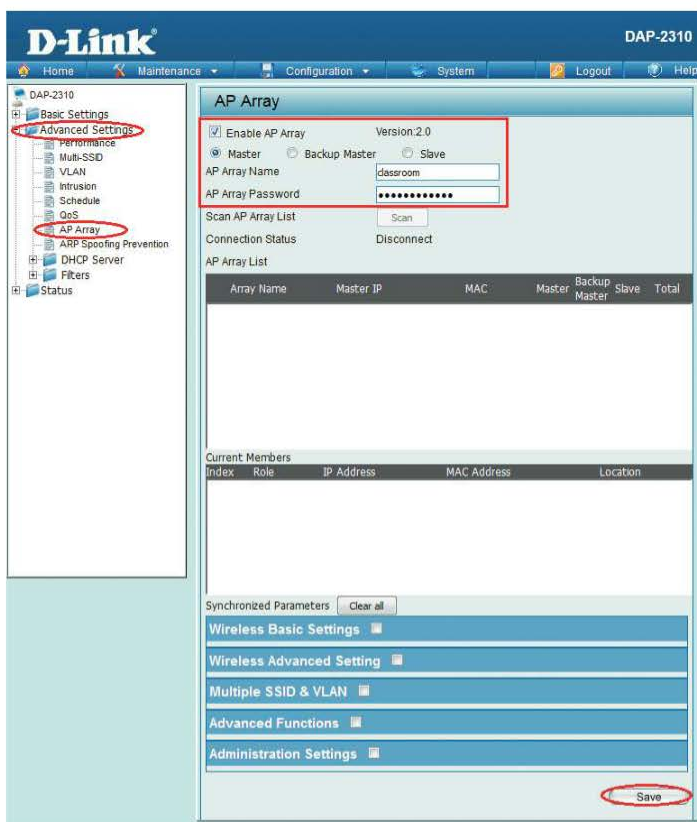


Рис. 11.2. Настройка ведущей точки доступа

Шаг 3. Сохраните и активируйте настройки. Выберите *Configuration* → *Save and Activate*.

Настройка точки доступа AP2

Шаг 1. Зайдите на Web-интерфейс точки доступа AP2 и уменьшите выходную мощность передатчика точки доступа до 12,5 %.

Шаг 2. Настройте точку доступа AP2 резервной ведущей (backup master) в группе AP Array. Для этого выберите *Advanced Settings* → *AP Array*, установите галочку *Enable AP Array* и переключатель *Backup Master*, в поле *AP Array Name* введите *classroom*, в поле *AP Array Password* введите *DlinkPassword*. Нажмите кнопку *Save* (рис. 11.3).

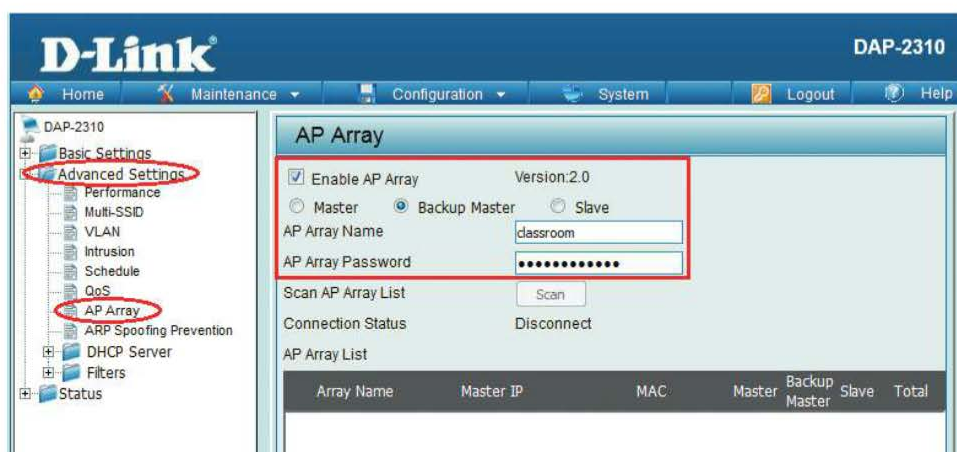


Рис. 11.3. Настройка резервной ведущей точки доступа

Шаг 3. Сохраните и активируйте настройки. Выберите *Configuration* → *Save and Activate*.

Настройка точки доступа AP3

Шаг 1. Зайдите на Web-интерфейс точки доступа AP3 и уменьшите выходную мощность передатчика точки доступа до 12,5 %.

Шаг 2. Настройте точку доступа AP3 ведомой (slave) в группе AP Array. Для этого выберите *Advanced Settings* → *AP Array*, установите галочку *Enable AP Array* и переключатель *Slave*, в поле *AP Array Name* введите *classroom*, в поле *AP Array Password* введите *DlinkPassword* и нажмите кнопку *Save* (рис. 11.4).

Шаг 3. Сохраните и активируйте настройки. Выберите *Configuration* → *Save and Activate*.

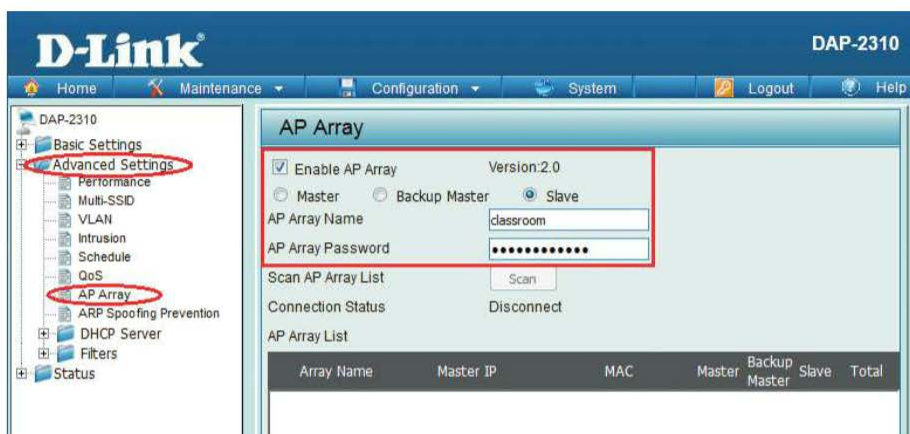


Рис. 11.4. Настройка ведомой точки доступа

Проверка работоспособности сети

Шаг 1. Просмотрите, какие точки доступа входят в созданную группу AP Array. Для этого зайдите на Web-интерфейс точки доступа AP1, выберите *Advanced Settings* → *AP Array*. В окне *Current Members* указаны все точки доступа, которые входят в группу *classroom*, и их роли (рис. 11.5).

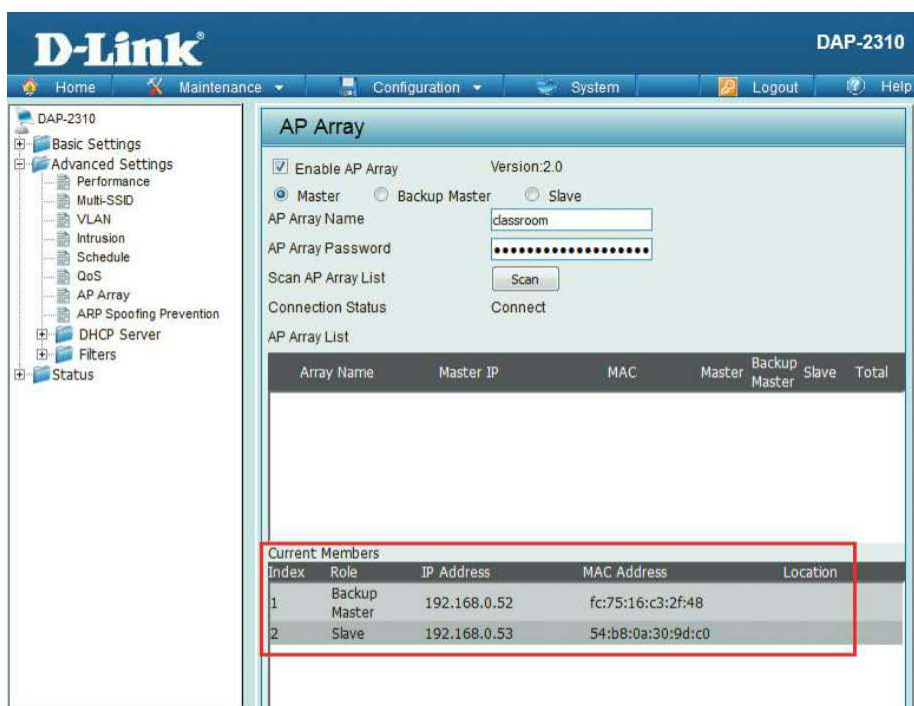


Рис. 11.5. Точки доступа, которые являются членами группы classroom

Шаг 2. На точке доступа AP1 создайте беспроводную сеть с SSID *Dlink_N*. Для этого:

- 1) выберите раздел *Basic Settings* → *Wireless*;
- 2) в списке *Mode* выберите *Access Point*;
- 3) в поле *Network Name (SSID)* введите *Dlink_N*;
- 4) отключите автоматический выбор канала. В поле *Auto Channel Selection* выберите *Disable*;
- 5) в поле *Channel* выберите 6;
- 6) в выпадающем меню *Authentication* выберите *WPA-Personal*;
- 7) в поле *PassPhrase* введите пароль *DlinkQwerty* и повторите его в поле *Confirm PassPhrase*;
- 8) сохраните настройки, нажав кнопку *Save*.

Шаг 3. Сохраните и активируйте настройки.

Шаг 4. Проверьте настройки беспроводной сети на точках доступа AP2 и AP3. Зайдите на Web-интерфейс точек доступа AP2 и AP3 в раздел *Status* → *Device Information* (рис. 11.6).



Рис. 11.6. Информация о настройках точки доступа

Какая беспроводная сеть настроена на точках доступа AP2 и AP3? _____
Точки доступа AP2 и AP3 синхронизировали настройки с ведущей точкой доступа? _____

Шаг 5. На точке доступа AP3 измените SSID беспроводной сети на *Class_N*.

Шаг 6. Сохраните и активируйте настройки.

Изменилось название беспроводной сети на точках доступа AP1 и AP2 на *Class_N*? Объясните почему? _____

Проверьте настройки точки доступа AP2. Что вы наблюдаете? _____

Лабораторная работа № 12. Сегментация беспроводной сети на основе двухдиапазонных точек доступа

При поддержке точкой доступа или маршрутизатором одновременной работы в диапазонах 2,4 и 5 ГГц наилучшим решением является использование сразу обоих диапазонов: низкоскоростных клиентов стандартов 802.11g или 802.11n можно подключать к сети в диапазоне 2,4 ГГц, высокоскоростных клиентов 802.11n или 802.11ac — в диапазоне 5 ГГц. Это позволит физически «разделить» клиентов, избежать «конфликтов» между ними и повысить производительность сети.

Дополнительно к сегментации по частотным диапазонам можно выполнять сегментацию на основе SSID, привязанным к разным VLAN стандарта 802.1Q.

Оборудование (на 1 рабочее место):

Рабочая станция	3 шт.
Беспроводной адаптер DWA-160 или DWA-582	2 шт.
Беспроводной адаптер DWA-182	1 шт.
Точка доступа DAP-2660	1 шт.
Кабель Ethernet	1 шт.

Цель работы: научиться настраивать сегментацию сети на точке доступа DAP-2660.

Перед выполнением задания (рис. 12.1) верните настройки точки доступа к заводским настройкам по умолчанию.

Примечание. Настройка точки доступа выполняется с рабочей станции ПК 1.

Шаг 1. Подключите Ethernet-кабель к LAN-порту точки доступа и к сетевому адаптеру рабочей станции ПК 1.

Шаг 2. Настройте статический IP-адрес на Ethernet-адаптере рабочей станции ПК 1 — 192.168.0.1 с маской подсети 255.255.255.0.

Шаг 3. Зайдите на Web-интерфейс точки доступа. Измените IP-адрес управления на 192.168.N.50 с маской подсети 255.255.255.0. Сохраните и активируйте настройки.

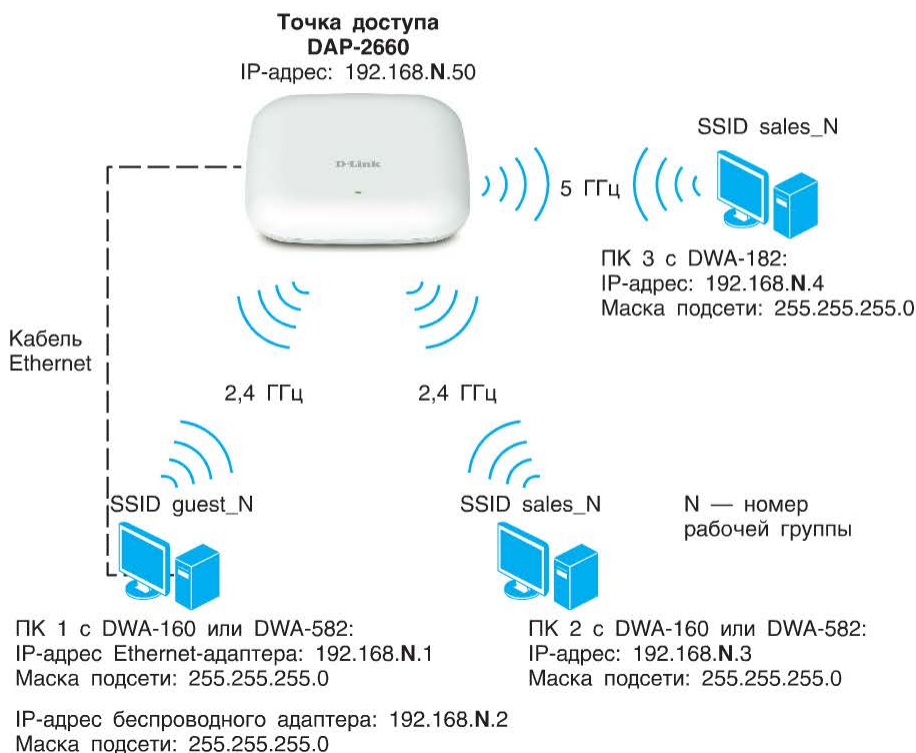


Рис. 12.1. Общая схема сети

Шаг 4. Измените IP-адрес Ethernet-адаптера рабочей станции ПК 1 на 192.168.N.1 с маской подсети 255.255.255.0.

Шаг 5. Уменьшите выходную мощность передатчика точки доступа до 12,5 %.

Шаг 6. Создайте сегмент сети с SSID *guest_N* в диапазоне частот 2,4 ГГц. Для этого:

- 1) выберите раздел *Basic Settings* → *Wireless*;
- 2) в выпадающем списке *Wireless Band* выберите *2.4 GHz*;
- 3) в поле *Mode* выберите *Access Point*;
- 4) в поле *Network Name (SSID)* введите *guest_N*;
- 5) отключите автоматический выбор канала. В поле *Auto Channel Selection* выберите *Disable*;
- 6) в поле *Channel* выберите *6*;
- 7) в выпадающем меню *Security* выберите *WPA-Personal*;
- 8) в поле *PassPhrase* введите *DlinkPassword* и повторите его в поле *Confirm PassPhrase*;
- 9) сохраните настройки, нажав кнопку *Save* (рис. 12.2).

Шаг 7. Создайте сегмент сети с SSID *sales_N* в диапазоне частот 5 ГГц. Для этого:



Рис. 12.2. Создание сегмента сети с SSID guest_0 в диапазоне 2,4 ГГц

- 1) выберите раздел *Basic Settings* → *Wireless*;
- 2) в выпадающем списке *Wireless Band* выберите *5 GHz*;
- 3) в поле *Mode* выберите *Access Point*;
- 4) в поле *Network Name (SSID)* введите *sales_N*;
- 5) отключите автоматический выбор канала. В поле *Auto Channel Selection* выберите *Disable*;
- 6) в поле *Channel* выберите *36*;
- 7) в выпадающем меню *Security* выберите *WPA-Personal*;
- 8) в поле *PassPhrase* введите *PasswordLink* и повторите его в поле *Confirm PassPhrase*;
- 9) сохраните настройки, нажав кнопку *Save* (рис. 12.3).

Шаг 8. Сохраните и активируйте настройки. Для этого выберите *Configuration* → *Save and Activate*.

Шаг 9. Настройте статические IP-адреса на беспроводных интерфейсах ПК 1 и ПК 3, как показано на рис. 12.1.

Шаг 10. Рабочую станцию ПК 1 подключите к беспроводной сети *guest_N*, рабочую станцию ПК 3 — к *sales_N*.

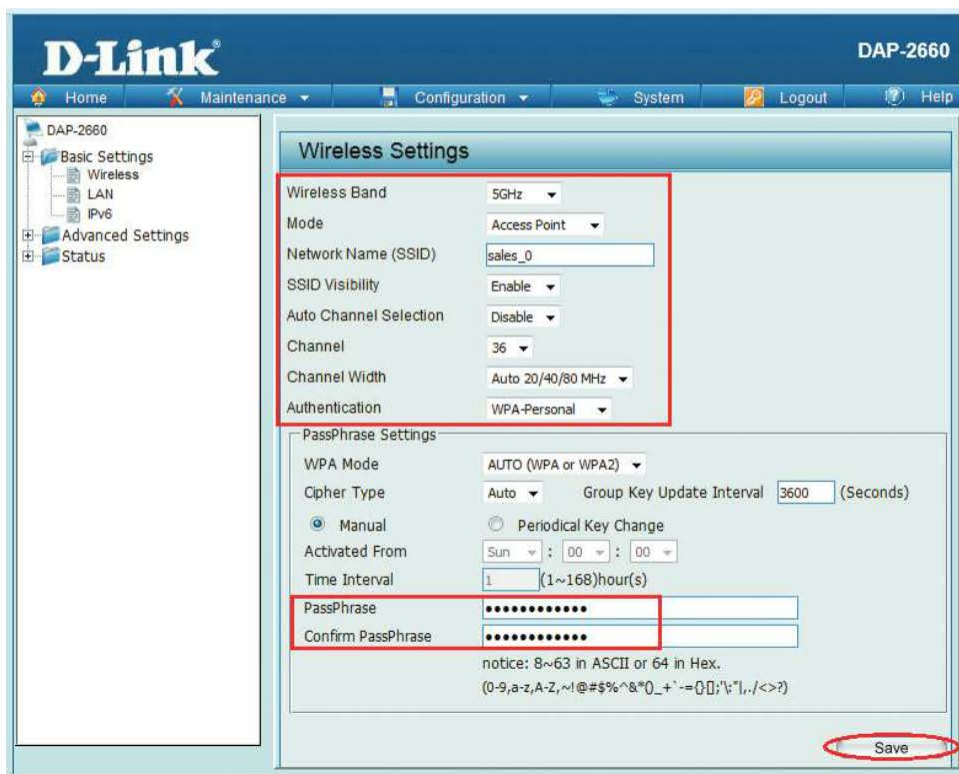


Рис. 12.3. Создание сегмента сети с SSID sales_0 в диапазоне 5 ГГц

Шаг 11. Проверьте доступность соединения между рабочими станциями командой ping:

от ПК 1 к ПК 3 _____

от ПК 3 к ПК 1 _____

Объясните наличие/отсутствие связи между рабочими станциями _____

Шаг 12. Отключитесь от беспроводных сетей *guest_N* и *sales_N*.

Шаг 13. Создайте сегмент беспроводной сети с SSID *sales_N* в диапазоне частот 2,4 ГГц. Для этого:

- 1) зайдите во вкладку *Advanced Settings* → *Multi-SSID*;
- 2) в выпадающем списке *Band* выберите *2.4 GHz*;
- 3) активируйте функцию *Multi-SSID* для частотного диапазона 2,4 ГГц, поставив галочку в *Enable Multi-SSID*;
- 4) в выпадающем списке *Index* выберите *SSID1*;
- 5) в поле *SSID* введите *sales_N*;

- 6) в выпадающем меню *Security* выберите *WPA-Personal*;
 - 7) в поле *PassPhrase* введите *PasswordLink* и повторите его в поле *Confirm PassPhrase*;
 - 8) нажмите кнопку *Add* (рис. 12.4).
- Сохраните созданные сегменты, нажав кнопку *Save* (рис. 12.5).

Рис. 12.4. Создание сегмента сети с SSID sales_0 в диапазоне 2,4 ГГц

Index	SSID	Band	Encryption	Delete
Primary SSID	guest_0	2.4 GHz	WPA2-Auto-Personal	
Multi-SSID1(Edit)	sales_0	2.4 GHz	WPA2-Auto-Personal	

Save

Рис. 12.5. Созданные сегменты с SSID sales_0 и SSID guest_0 в диапазоне 2,4 ГГц

Шаг 14. Настройте привязку SSID и VLAN. Трафик беспроводной сети с *SSID guest_N* должен направляться в *VLAN guest_N* (VID 20), а беспроводной сети с *SSID sales_N* — в *VLAN sales_N* (VID 10). MSSID-порты *Primary* 5 ГГц и *S-1* 2,4 ГГц являются немаркированными портами *VLAN sales_N*. MSSID-порт *Primary* 2,4 ГГц является немаркированным портом *VLAN guest_N*. Для этого:

1) зайдите во вкладку *Advanced Settings* → *VLAN* и включите поддержку VLAN, выбрав *Enable* в поле *VLAN Status*. Нажмите кнопку *Save*;

2) удалите порты из VLAN по умолчанию (default). Во вкладке *VLAN List* нажмите *Edit*;

3) в открывшемся окне установите галочки *Not Member* для MSSID-портов *Primary* и *S-1* в диапазоне 2,4 ГГц и для *Primary* в диапазоне 5 ГГц. Нажмите кнопку *Save*;

4) выберите вкладку *Add/Edit VLAN*. В поле *VLAN ID (VID)* введите *10*, в поле *VLAN Name* — *sales_N*. MSSID-порты *Primary* 5 ГГц и *S-1* 2,4 ГГц включите в VLAN как немаркированные. Остальные MSSID-порты отметьте как *Not Member*. Нажмите кнопку *Save* (рис. 12.6).

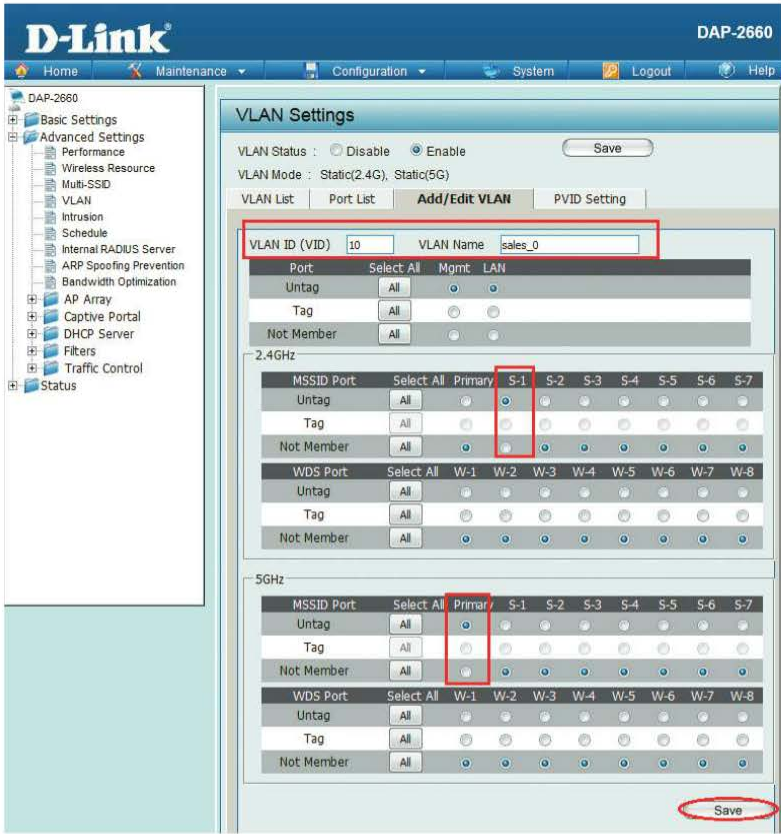


Рис. 12.6. Создание VLAN sales_0

Аналогичным образом создайте *VLAN guest_N* с *VID 20*. *MSSID*-порт *Primary* 2,4 ГГц включите в *VLAN* как немаркированный. Остальные *MSSID*-порты отметьте как *Not Member*. Нажмите кнопку *Save* (рис. 12.7).

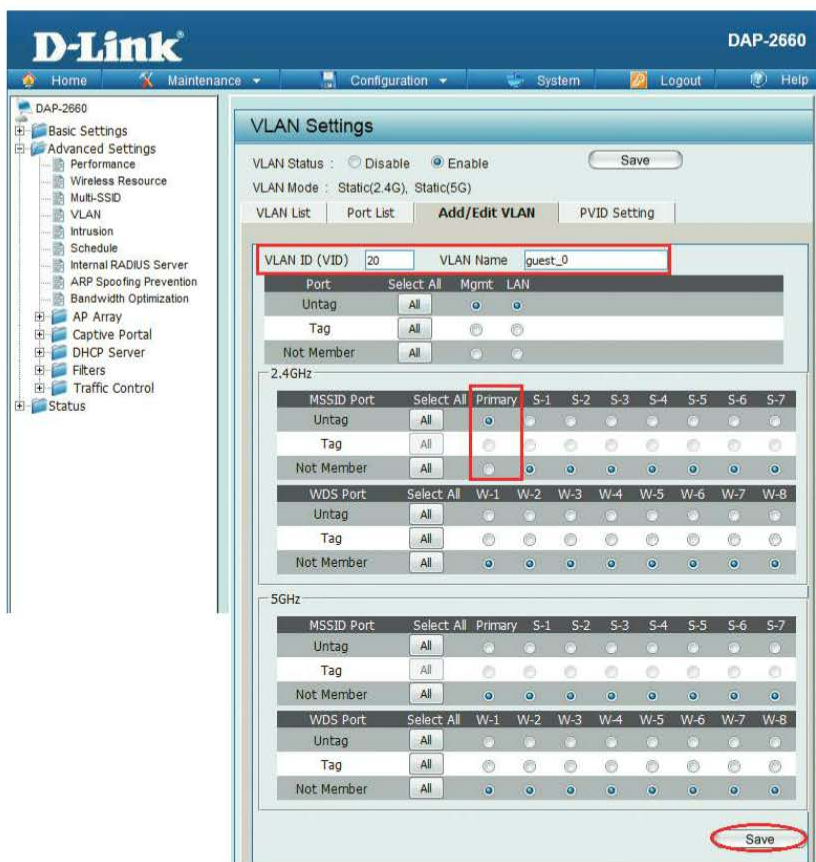


Рис. 12.7. Создание VLAN guest_0

Шаг 15. Просмотрите созданные VLAN. Для этого зайдите во вкладку *Advanced Settings* → *VLAN* → *VLAN List*.

Шаг 16. Назначьте PVID немаркированным *MSSID*-портам. Для этого выберите вкладку *PVID Setting*. В полях *S-1* для 2,4 ГГц и *Primary* для 5 ГГц введите 10, в поле *Primary* для 2,4 ГГц — 20. Нажмите кнопку *Save*.

Шаг 17. Для того чтобы двухдиапазонное клиентское оборудование подключалось к точке доступа в диапазоне 5 ГГц, настройте функцию *Band Steering*. Для этого зайдите во вкладку *Advanced Settings* → *Wireless Resource*. В выпадающем меню *Wireless Band* выберите *5 GHz*, в *Band Steering* → *Enable*. Нажмите кнопку *Save* (рис. 12.8).

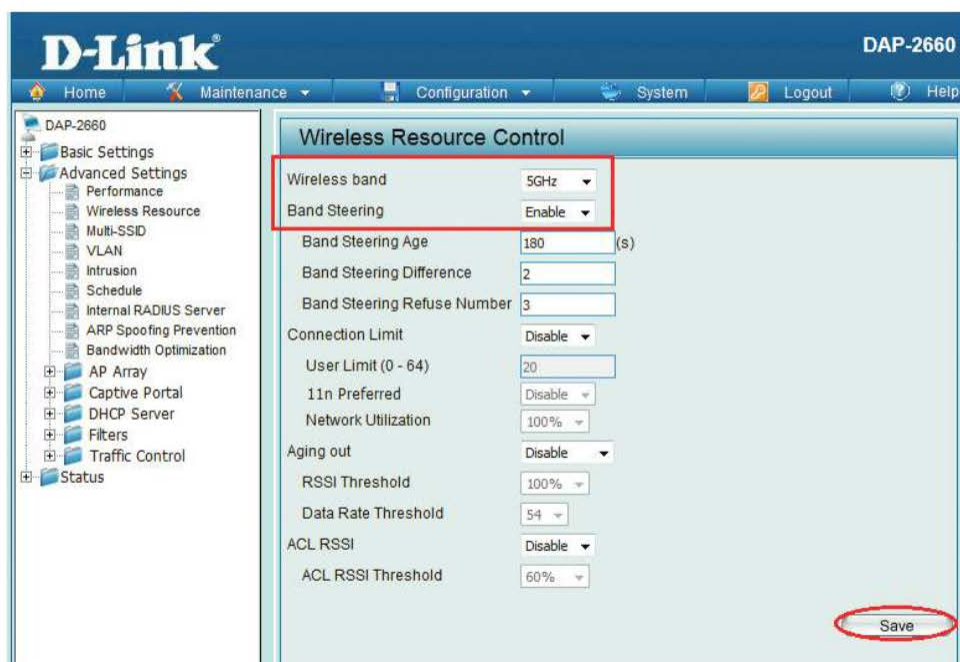


Рис. 12.8. Настройка функции *Band Steering*

Шаг 18. Сохраните и активируйте настройки. Для этого выберите *Configuration* → *Save and Activate*.

Шаг 19. Настройте статический IP-адрес на беспроводном интерфейсе ПК 2.

Шаг 20. Отключите Ethernet-кабель от точки доступа.

Шаг 21. Рабочую станцию ПК 1 подключите к беспроводной сети *guest_N*, рабочие станции ПК 2 и ПК 3 — к *sales_N*.

Шаг 22. Проверьте доступность соединения между рабочими станциями командой *ping*:

от ПК 1 к ПК 2 и ПК 3 _____

от ПК 2 к ПК 1 и ПК 3 _____

от ПК 3 к ПК 1 и ПК 2 _____

Объясните наличие/отсутствие связи между рабочими станциями _____

Лабораторная работа № 13.

Настройка программного контроллера CWM-100

Central WifiManager CWM-100 представляет собой программный контроллер для централизованного управления автономными точками доступа серии DAP-xxx. С помощью CWM-100 администратор сети может управлять большим количеством точек доступа (до 1000), находясь как непосредственно в сети, так и за ее пределами (удаленно). В отличие от аппаратных контроллеров CWM-100 не требует приобретения дополнительных лицензий для увеличения числа управляемых точек доступа при расширении сети.

Функции Central WifiManager и AP Array являются взаимно исключаящими. Автономная точка доступа может быть под управлением только одной из этих функций.

Программное обеспечение контроллера может быть установлено как на компьютер под управлением Microsoft Windows, так и на удаленную облачную платформу. ПО доступно бесплатно на сайте компании D-Link (www.dlink.ru).

В решение Central WiFiManager входят следующие компоненты: сервер Central WiFiManager (CWM-сервер); модули управления точками доступа; утилита для обнаружения точек доступа.

Программный контроллер позволяет выполнять в беспроводной сети настройку следующих функций: аутентификацию пользователей с использованием локальной базы данных и внешних серверов RADIUS, LDAP, POP3; реализацию портала аутентификации пользователей хот-спота (публичной беспроводной сети); реализацию портала аутентификации при гостевом доступе; автоматическое управление выходной мощностью точек доступа; автоматический выбор канала точками доступа; самовосстановление зоны покрытия в результате выхода из строя точки доступа за счет увеличения мощности соседних; балансировку нагрузки между диапазонами двухдиапазонных точек доступа; обнаружение несанкционированных точек доступа.

Оборудование (на 1 рабочее место):

Рабочая станция 1 шт.

Точка доступа DAP-2660 1 шт.

Кабель Ethernet 1 шт.

ПО — централизованное управление точками доступа Central WiFiManager

Цель работы: изучить базовые настройки программного контроллера Central WiFiManager.

Перед выполнением задания (рис. 13.1) верните настройки точки доступа к заводским настройкам по умолчанию.

Шаг 1. Подключите Ethernet-кабель к LAN-порту точки доступа и к сетевому адаптеру рабочей станции ПК.

Шаг 2. Настройте статический IP-адрес на Ethernet-адаптере рабочей станции ПК — 192.168.0.1 с маской подсети 255.255.255.0.

Точка доступа
DAP-2660
IP-адрес: 192.168.N.50



Кабель Ethernet



ПК с CWM-100:
IP-адрес: 192.168.N.98
Маска подсети: 255.255.255.0

Рис. 13.1. Схема сети

Шаг 3. Зайдите на Web-интерфейс точки доступа. Измените IP-адрес управления на 192.168.N.50 с маской подсети 255.255.255.0. Сохраните и активируйте настройки.


Шаг 4. Измените IP-адрес Ethernet-адаптера рабочей станции ПК на 192.168.N.98 с маской подсети 255.255.255.0.

Шаг 5. Уменьшите выходную мощность передатчика точки доступа до 12,5 %.

Шаг 6. Установите программное обеспечение CWM-100 на ПК. Для этого запустите установщик и следуйте инструкциям мастера установки.

Шаг 7. Запустите мастер установки модуля для DAP-2660.

Примечание. Список точек доступа серии DAP-xxxx, которые поддерживают работу с Central WiFiManager, указан в описании контроллера на сайте компании.

Шаг 8. Запустите работу Central WiFiManager Server, дважды щелкнув левой кнопкой мыши по соответствующему значку на рабочем столе. Затем нажмите кнопку  в открывшемся диалоговом окне (рис. 13.2).

Шаг 9. Зайдите на Web-интерфейс контроллера Central WiFiManager. Для этого нажмите соответствующий значок на рабочем столе Windows. В открывшейся странице авторизации введите имя пользователя, пароль (по умолчанию имя пользователя — *admin*, пароль — *admin*) и код идентификации CAPTCHA (с учетом регистра) (рис. 13.3).

Шаг 10. Проверьте список точек доступа, для которых были установлены модули управления. Для этого выберите раздел *Система* → *Модуль* (рис. 13.4).

Шаг 11. Задайте адрес, по которому будет доступен Central WiFiManager. Для этого перейдите во вкладку *Система* → *Общий*. В поле *Адрес доступа* введите 192.168.N.98 и нажмите кнопку *Ок* (рис. 13.5). Перезапустите Central WiFiManager Server.

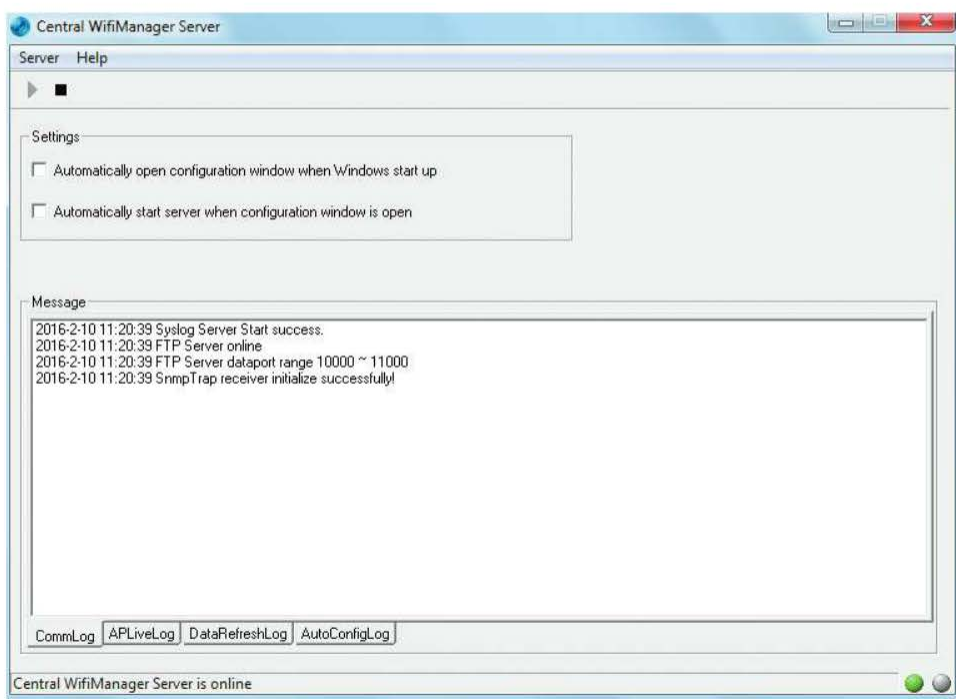


Рис. 13.2. Запуск Central WiFiManager Server

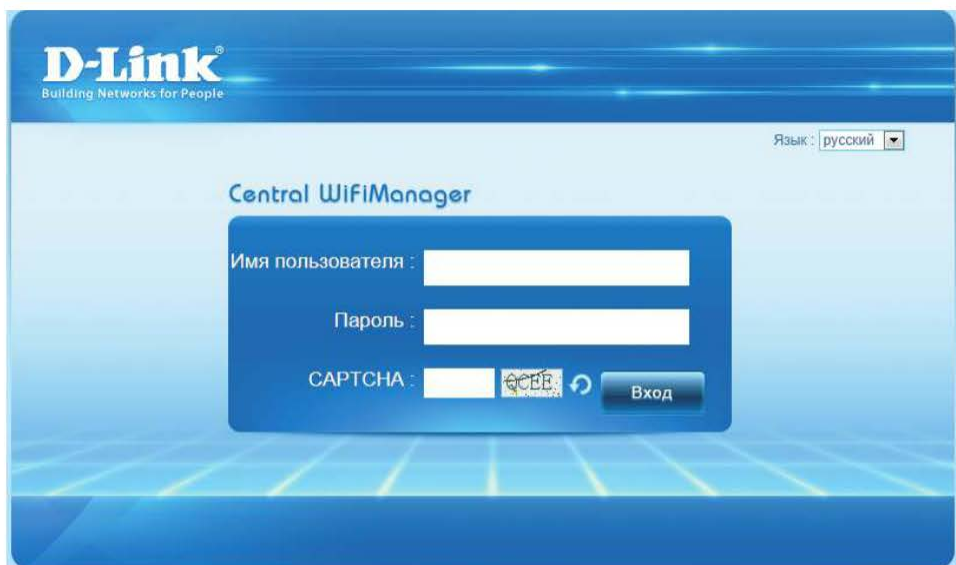


Рис. 13.3. Окно авторизации Central WiFiManager

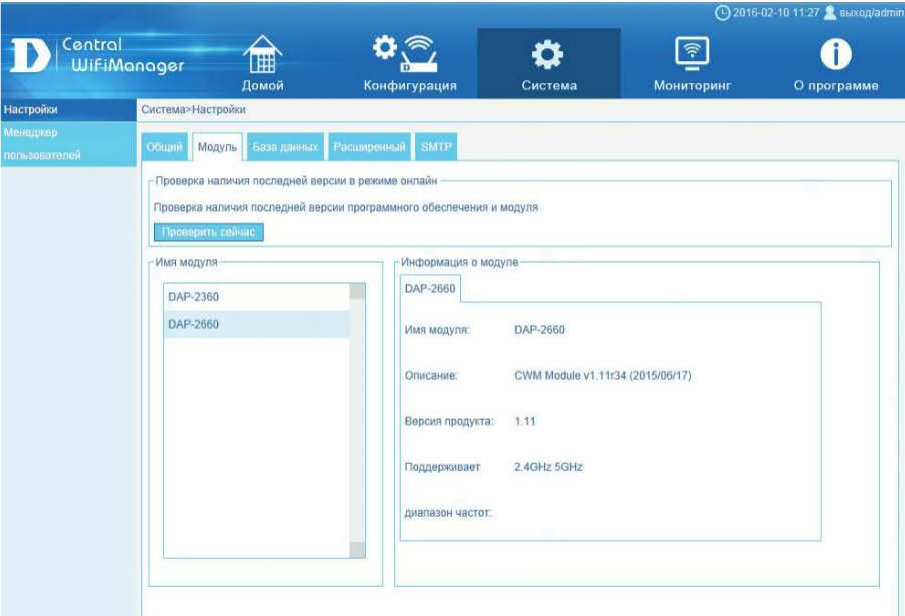


Рис. 13.4. Установленные модули управления

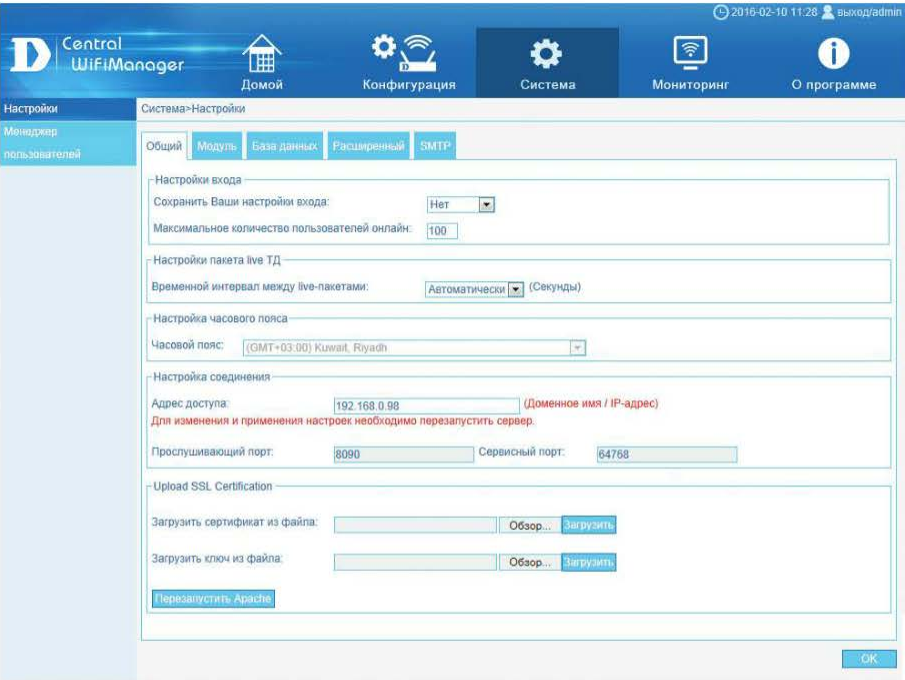



Рис. 13.5. Изменение адреса доступа для Central WiFiManager

Шаг 12. Создайте объект, к которому будут относиться управляемые через программный контроллер точки доступа. Для этого в разделе *Конфигурация* в меню слева выберите раздел *Объект* и нажмите кнопку  в правом верхнем углу страницы (рис. 13.6). В поле *Имя объекта* введите *D-Link* и нажмите кнопку ОК (рис. 13.7, 13.8).

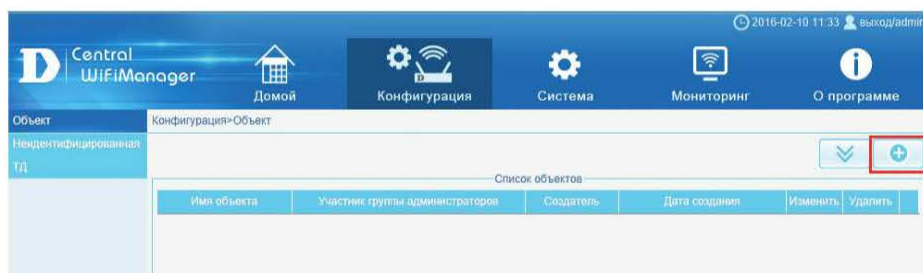


Рис. 13.6. Создание объекта

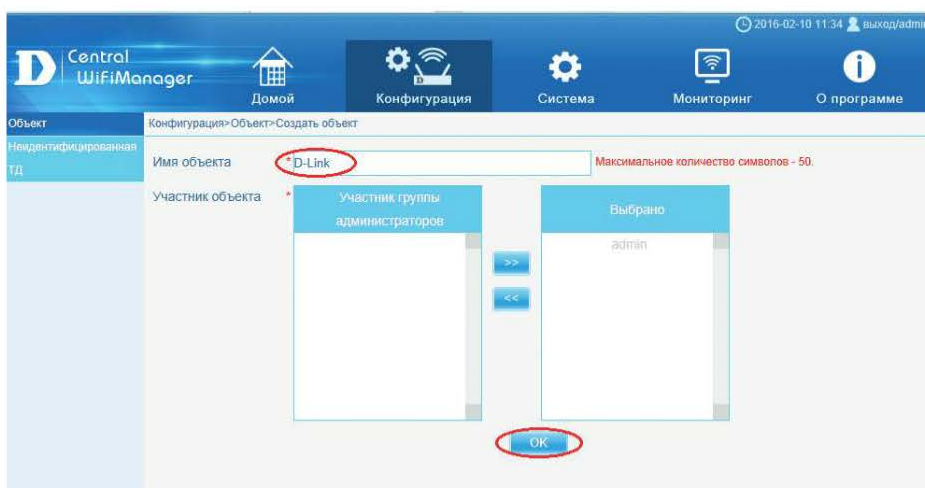


Рис. 13.7. Создание объекта D-Link

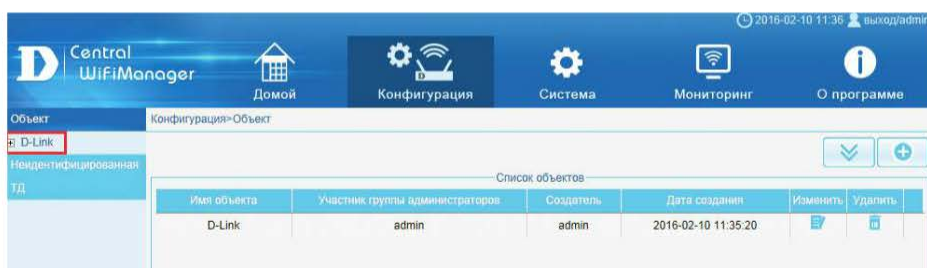



Рис. 13.8. Объект D-Link

Шаг 13. Добавьте сетевой профиль для объекта D-Link. Для этого в меню слева выберите профиль D-Link (1), на открывшейся странице нажмите кнопку  (2) (рис. 13.9).

В поле *Имя сети* введите *SSID_N* и нажмите кнопку ОК (рис. 13.10).

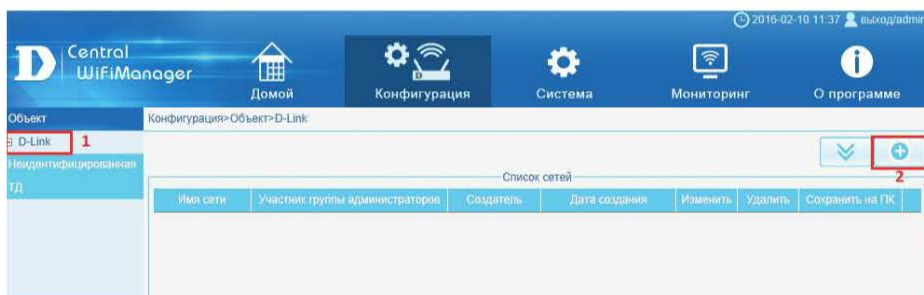


Рис. 13.9. Создание сетевого профиля для объекта D-Link

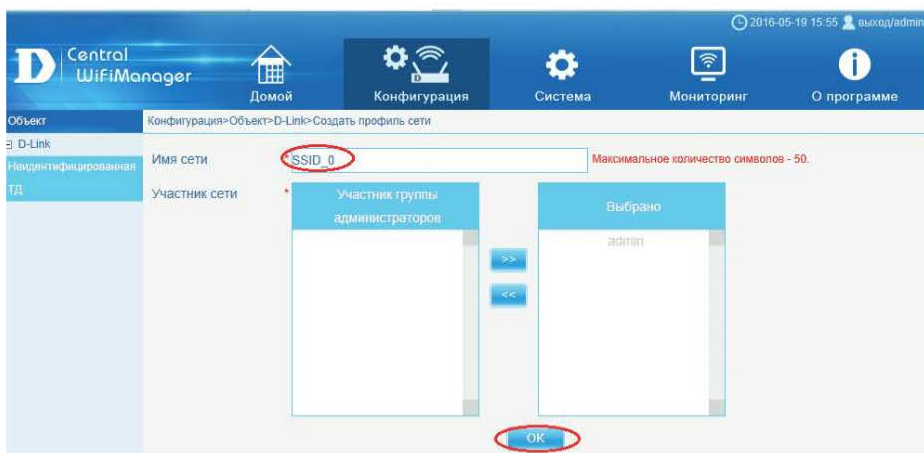

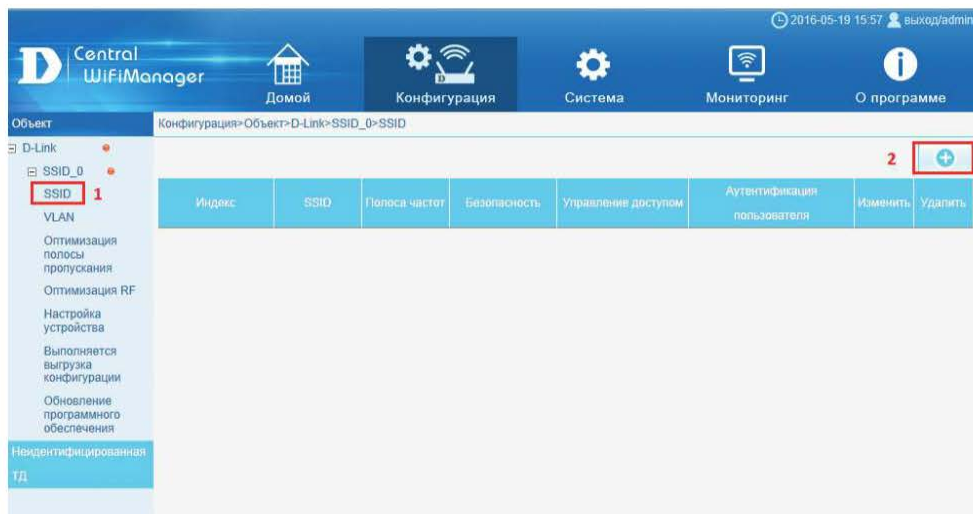


Рис. 13.10. Создание сетевого профиля SSID_0

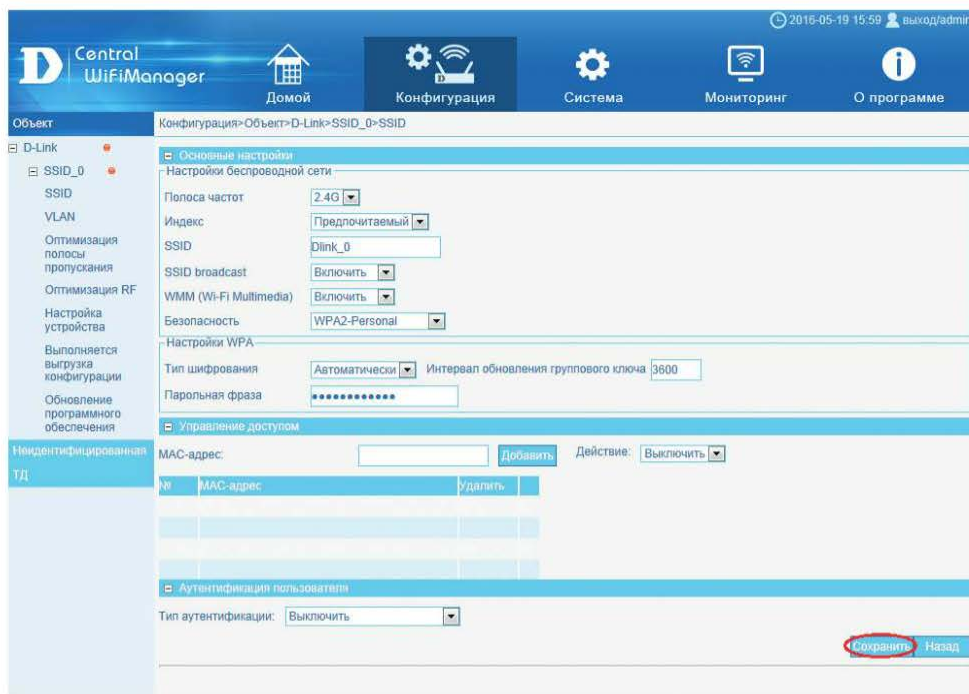
Шаг 14. Настройте параметры беспроводной сети. В меню слева выберите SSID (1) и нажмите кнопку  (2) (рис. 13.11, а).

В открывшемся окне в поле *SSID* введите *Dlink_N*, в списке *Безопасность* выберите *WPA2-Personal*, в поле *Парольная фраза* введите *PasswordDlink*. Нажмите кнопку *Сохранить* (рис. 13.11, б).

Шаг 15. Добавьте точку доступа DAP-2660 в CWM-100. Для обнаружения и добавления точек доступа используется утилита *AP installation utility for CWM*, входящая в комплект ПО Central WiFiManager. Загрузите на ПК утилиту — в разделе *Конфигурация* нажмите кнопку  (рис. 13.12). После загрузки распакуйте архив и запустите *AP installation utility for CWM.exe*. Для обнаружения точек доступа нажмите *Обнаружить* (рис. 13.13).



а



б

Рис. 13.11. Создание параметров для SSID_0

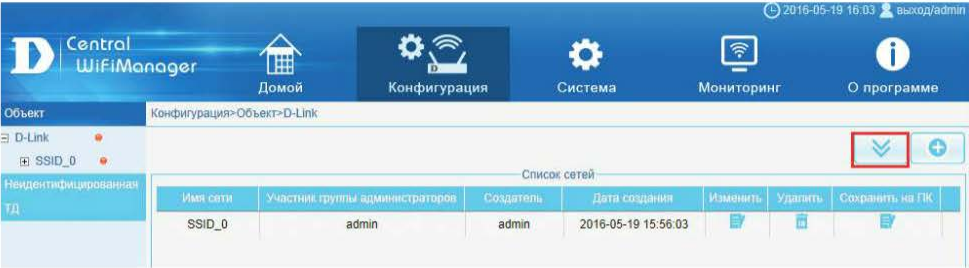


Рис. 13.12. Загрузка утилиты для обнаружения точек доступа

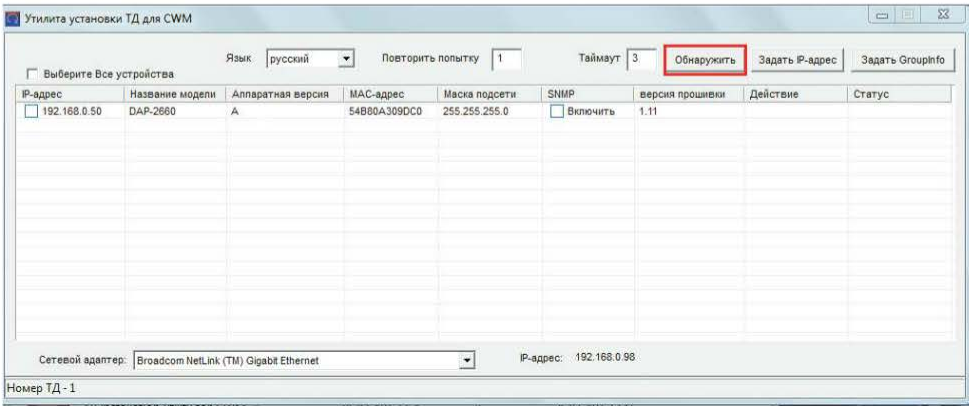


Рис. 13.13. Обнаружение точек доступа

Для добавления точки доступа в Central WiFiManager необходимо загрузить на нее сетевой профиль, созданный на шаге 13. Этот файл содержит в себе информацию о ключе аутентификации и IP-адрес контроллера. Для того чтобы загрузить сетевой профиль на ПК, перейдите в раздел *Конфигурация*, выберите профиль *SSID_N* и нажмите *Сохранить на ПК* (рис. 13.14).

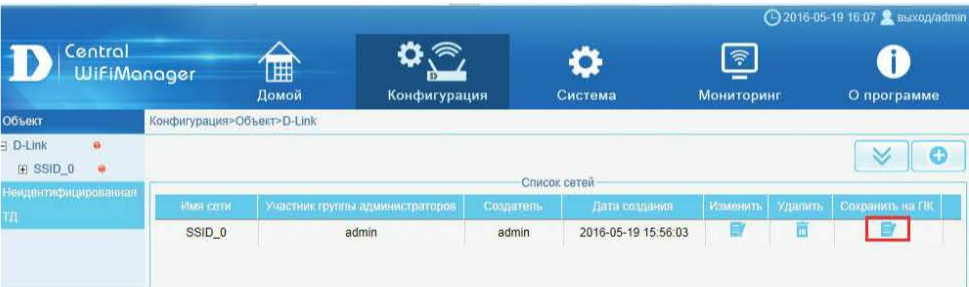


Рис. 13.14. Сохранение сетевого профиля на ПК

Вернитесь к утилите для обнаружения точек. Установите галочку напротив DAP-2660 и нажмите *Задать GroupInfo* (рис. 13.15).



Рис. 13.15. Загрузка профиля на точку доступа

В открывшемся окне в поле *Файл* укажите загруженный файл с профилем, после чего проверьте доступность сервера, нажав кнопку *Тест*.

Примечание. Проверка осуществляется путем обращения ПК, на котором запущена утилита обнаружения точек доступа, на IP-адрес, указанный в поле *Адрес доступа* на странице *Система* → *Общие*.

После проверки нажмите кнопку *Определять* (рис. 13.16).

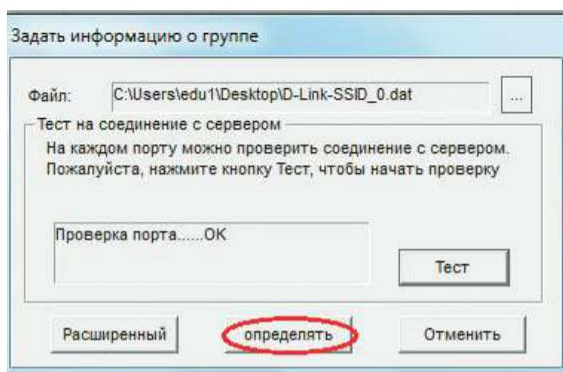


Рис. 13.16. Проверка доступности CWM-сервера

После того как в колонке *Статус* (рис. 13.17) отобразится надпись *Успех*, точка доступа DAP-2660 появится в Web-интерфейсе Central WiFiManager.

Проверьте, добавилась ли точка доступа в CWM-100. Перейдите на страницу *Домой* → *Объект* (рис. 13.18).

Шаг 16. Загрузите параметры беспроводной сети на точку доступа. Перейдите на страницу *Конфигурация* → *SSID_N* → *Выполняется выгрузка конфигурации*. Нажмите *Завершить* (рис. 13.19).



Рис. 13.17. Добавление DAP-2660 в CWM-100

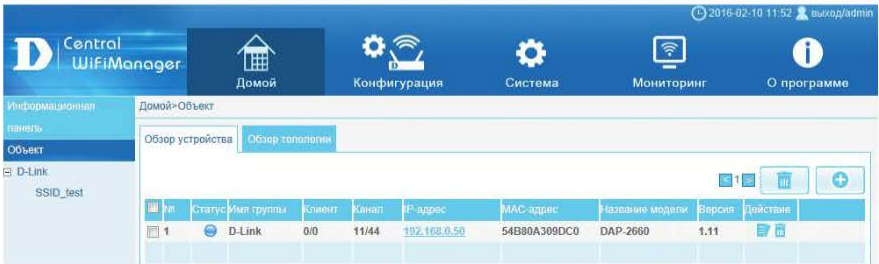


Рис. 13.18. Информация о точке доступа, управляемой через CWM-100

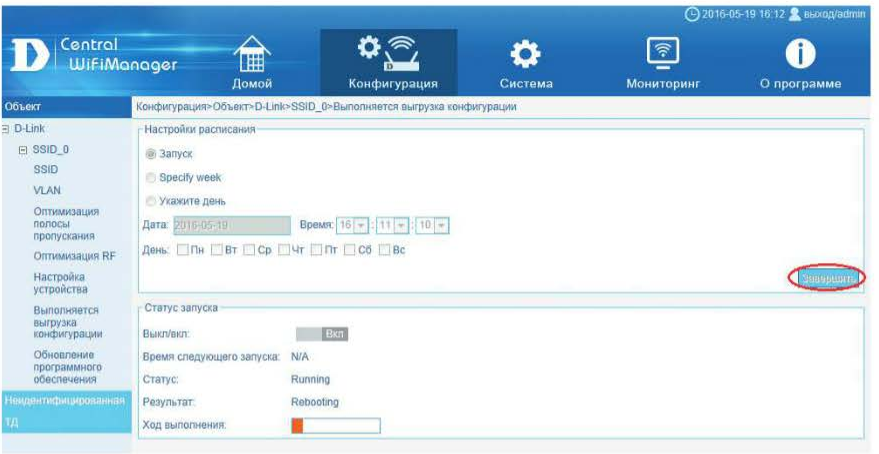


Рис. 13.19. Загрузка параметров беспроводной сети на точку доступа

Шаг 17. Убедитесь, что параметры беспроводной сети загружены на точку доступа. Зайдите на Web-интерфейс точки доступа в раздел *Status* → *Device Information*.

Литература

1. IEEE Std 802.11™—2012. IEEE Standard for Information technology — Telecommunications and information exchange between systems Local and metropolitan area networks — Specific requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.
2. IEEE Std 802.11ac™—2013. IEEE Standard for Information technology — Telecommunications and information exchange between systems Local and metropolitan area networks — Specific requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment 4: Enhancements for Very High Throughput for Operation in Bands below 6 GHz.
3. Столлингс В. Беспроводные линии связи и сети: пер. с англ. М.: Издательский дом «Вильямс», 2003.
4. Stallings W. Cryptography and Network Security. Principles and Practice. Fifth Edition. Prentice Hall, 2011.
5. Gast M. 802.11n: A Survival Guide. O'Reilly Media, 2012.
6. Gast M. 802.11ac: A Survival Guide. O'Reilly Media, 2013.
7. Geier J. Designing and Deploying 802.11 Wireless Networks: A Practical Guide to Implementing 802.11n and 802.11ac Wireless Networks, Second Edition. Cisco Press, 2015.
8. Wi-Fi CERTIFIED for WMM — Support for Multimedia Applications with Quality of Service in Wi-Fi Networks. Wi-Fi Alliance. September 1, 2004.
9. Wi-Fi CERTIFIED Wi-Fi Protected Setup: Easing the User Experience for Home and Small Office Wi-Fi Networks. Wi-Fi Alliance Originally Published. December 2010. Updated March 2014.
10. Designed for Speed: Network Infrastructure in an 802.11n World. White Paper. Aruba Networks, 2013.
11. 802.11ac In-Depth. White Paper. Aruba Networks, 2014.
12. Wi-Fi Alliance Technical Committee 2 WMM-Admission Control Technical Task Group. Wi-Fi Multimedia Technical Specification 4 (with WMM-Power Save and WMM-Admission Control). Version 1.2.0. Wi-Fi Alliance, 2012.
13. Buettrich S. Itrainonline MMTK Radio Link Calculation Handout.
14. High-Density Wi-Fi Design Principles. White Paper. Aerohive Networks, 2012.
15. Florwick J., Whiteaker J., Amrod A.C., Woodhams J. Wireless LAN Design Guide for High Density Client Environments in Higher Education. Design Guide. Cisco systems, 2013.
16. Perahia E., Gong M.X. Gigabit Wireless LANs: an overview of IEEE 802.11ac and 802.11ad. Intel Corporation.
17. RFC 4118. Architecture Taxonomy for Control and Provisioning of Wireless Access Points (CAPWAP). June 2005.

ГЛОССАРИЙ

А

ACL (англ. Access Control List). Списки управления доступом. Являются средством фильтрации потоков данных. Используя ACL, можно ограничить типы приложений, разрешенных для использования в сети, контролировать доступ пользователей к ресурсам сети и определять устройства, к которым они могут подключаться. Также ACL могут использоваться для определения политики QoS путем классификации трафика и переопределения его приоритета.

AES (англ. Advanced Encryption Standard). Симметричный алгоритм блочного шифрования (размер блока 128 бит, ключ 128/192/256 бит). Инициатива в разработке алгоритма AES принадлежит Национальному институту стандартов и технологий (NIST) США. В результате длительного процесса оценки предложенных алгоритмов в качестве AES был выбран алгоритм Rijndael. AES определен в FIPS PUB 197–2001. Адаптирован под требования многих протоколов, включая протокол CCMP (CTR with CBC-MAC Protocol) для сетей 802.11.

Access layer. Уровень доступа. Является нижним уровнем иерархической модели сети и управляет доступом пользователей и рабочих групп к ресурсам объединенной сети. Основной задачей уровня доступа является создание точек входа/выхода пользователей в сеть.

Access point. Точка доступа. Любой объект, обладающий функциональными возможностями станции и обеспечивающий доступ к распределительной системе (DS) посредством беспроводной среды.

Active scanning. Активное сканирование. Функция обнаружения точек доступа клиентами 802.11, отправляющими широкоэвещательные кадры пробного запроса (Probe request) в каждый из проверяемых каналов.

Ad hoc mode. Режим ad hoc. Режим работы, при котором клиенты 802.11 могут взаимодействовать друг с другом напрямую без использования точек доступа. В режиме ad hoc работают только беспроводные адаптеры.

Analog signal. Аналоговый сигнал. Непрерывно изменяющиеся электромагнитные колебания, которые могут распространяться в различных средах.

Antenna. Антенна. Проводник (или система проводников), используемый для излучения и приема электромагнитных волн.

Antenna gain. Коэффициент усиления антенны. Является мерой направленности антенны, определяется как отношение мощности сигнала, излученного в определенном направлении, к мощности сигнала, излучаемого идеальной (изотропной) антенной в любом направлении.

Association. Ассоциация. Процесс, в результате выполнения которого станция 802.11 становится частью беспроводной локальной сети.

Attenuation. Затухание. Уменьшение значения тока, напряжения или мощности сигнала при передаче.

Authentication. Аутентификация. Сервис безопасности, обеспечивающий подтверждение получения информации от законного источника требуемым получателем.

Authorization. Авторизация. Предоставление прав и разрешений доступа индивидууму (или процессу), обеспечивающих возможность доступа к требуемому ресурсу. После того как пользователь аутентифицирован, авторизация определяет права, доступные пользователю.

В

Backbone. Магистраль. Часть сети, по которой передается основной трафик. Является чаще всего источником и приемником трафика других сетей.

Bandwidth. Полоса пропускания. Частотный диапазон сигналов, пропускаемых линией связи без значительных искажений. Измеряется в герцах (Гц).

Beamforming. Формирование диаграммы направленности. Метод, использующий сдвиг по времени (фазе) сигналов, передаваемых массивом антенн для фокусировки излучения в определенном направлении.

BPSK (англ. Binary Phase Shift Keying). Двухуровневая фазовая манипуляция. Метод модуляции, в котором для представления двух двоичных цифр используются две фазы несущего сигнала.

Bridge. Мост. Устройство, соединяющее две физические сети и передающее кадры из одной сети в другую. Работает на канальном уровне модели OSI.

Broadcast. Широковещание. Система доставки пакетов, в которой копия каждого пакета передается всем узлам, подключенным к сети.

Broadcast storm. Широковещательный шторм. Множество одновременных широковещательных рассылок в сети, которые, как правило, поглощают всю доступную полосу пропускания сети и могут вызвать ее отказ.

BSS (англ. Basic Service Set). Базовый набор услуг. Основной строительный блок беспроводной сети IEEE 802.11, состоящий из нескольких станций, реализующих общий протокол MAC и состоящих за доступ к разделяемой среде передачи.

BSSID (англ. Basic Service Set Identifier). Идентификатор базового набора услуг. Для BSS, работающего в инфраструктурном режиме, BSSID является MAC-адресом точки доступа. Для BSS, работающего в режиме ad hoc, BSSID является локально администрируемым MAC-адресом, генерируемым произвольным образом. BSSID всегда ассоциируется только с одним BSS и указывается в заголовке кадра данных.

Bus topology. Шинная топология. Топология сети, при которой все узлы равноправно подключаются к общей среде передачи.

С

Carrier frequency. Несущая частота. Непрерывная частота, модулируемая накладываемым информационным сигналом.

CCA (англ. Clear Channel Assessment). Логическая функция физического уровня 802.11, определяющая состояние текущей загрузки среды передачи.

CCMP (англ. Counter Mode Cipher Block Chaining Message Authentication Code Protocol, Counter Mode CBC-MAC Protocol). Протокол шифрования 802.11, основанный на AES.

Channel. Канал. Путь передачи сигналов между двумя или несколькими точками. Используются также термины: link, line, circuit и facility.

Client device. Клиентское устройство. Устройство, имеющее интерфейс, позволяющий использовать сервисы сети. Беспроводной клиент является одним из видов клиентских устройств.

Code rate. Скорость кодирования. В контексте сверточных кодов определяется как отношение числа бит данных к общему числу бит k/n . Показывает долю полезной информации в передаваемых данных.

Collision. Коллизия. Наложение или столкновение сигналов, возникающее во время одновременной передачи данных двумя или более узлами и приводящее к повреждению данных.

Coordination function. Функция координации. Логическая функция, определяющая момент времени, когда станция, функционирующая внутри базового набора услуг (BSS), может передавать PDU через беспроводную среду.

Core layer. Уровень ядра. Находится на самом верху иерархической модели сети и отвечает за надежную и быструю передачу больших объемов данных. Трафик, передаваемый через ядро, является общим для большинства пользователей. Сами пользовательские данные обрабатываются на уровне распределения, который, при необходимости, пересылает запросы к ядру.

CoS (англ. Class of Service). Класс обслуживания. Способ классификации и приоритизации пакетов на основе типа приложения или других методов классификации (802.1p, ToS, DiffServ) для обеспечения качества обслуживания в сети.

CSMA/CA (англ. Carrier Sense Multiple Access with Collision Avoidance). Метод множественного доступа с контролем несущей и предотвращением коллизий. Используется в качестве метода доступа к среде передачи в сетях 802.11. Уменьшает вероятность возникновения коллизий при одновременном доступе узлов к среде передачи.

D

Data confidentiality. Конфиденциальность данных. Сервис безопасности, обеспечивающий недоступность информации неавторизованным способом.

DBPSK (англ. Differential Binary Phase Shift Keying). Дифференциальная двух-уровневая фазовая манипуляция. Метод модуляции, при котором бит информации кодируется путем изменения фазы передаваемого сигнала. При передаче двоичного 0 фаза несущего сигнала не изменяется, при передаче двоичной 1 фаза несущего сигнала меняется на 180° .

DCF (англ. Distributed Coordination Function). Функция распределенной координации. Тип функции координации, при которой один и тот же алгоритм координации активен на каждой станции базового набора услуг (BSS) во время работы сети.

Decibel. Децибел. Мера сравнения двух сигналов. Обозначается дБ.

Diffserv (англ. Differentiated Services). Простой метод классификации, управления и предоставления качества обслуживания в современных IP-сетях. Использует для своей работы поле DSCP. Регламентируется RFC 2475, 3260.

Digital signal. Цифровой сигнал. Сигнал в дискретной или прерывистой форме.

Directional antenna. Направленная антенна. Антенна с направленной диаграммой направленности сигнала, излучающая сфокусированный электромагнитный луч в одном направлении.

Directional pattern (diagram). Диаграмма направленности антенны. Графическое представление характеристик излучения антенны как функции пространственных координат. Как правило, расстояние от антенны до любой точки диаграммы направленности пропорционально мощности, излучаемой антенной в этом направлении.

Distribution layer. Уровень распределения/агрегации. Средний уровень иерархической модели сети, который иногда называют уровнем рабочих групп, является связующим звеном между уровнями доступа и ядра.

DQPSK (англ. Differential Quadrature Phase Shift Keying). Дифференциальная квадратурная фазовая манипуляция. Метод модуляции, при котором бит информации кодируется путем изменения фазы передаваемого сигнала. DQPSK использует четыре значения фазы несущего сигнала (0° , 90° , 180° , 270°), и каждое состояние фазы выполняет передачу сразу двух бит последовательности (00, 01, 10, 11). Изменение фазы происходит при изменении информационных бит.

DS (англ. Distribution System). Распределительная система. Система, которая используется для соединения нескольких базовых наборов услуг (BSS) и интеграции проводной локальной сети в расширенный набор услуг (ESS).

DSCP (англ. Differentiated Services Code Point). Поле в заголовке IP-пакета, используемое для классификации (приоритизации) передаваемой информации. Регламентируется RFC 2774 и др.

DSSS (англ. Direct Sequence Spread Spectrum). Расширение спектра методом прямой последовательности. Разновидность технологий расширения спектра, в ко-

торой каждый бит исходного сигнала представляется несколькими битами передаваемого сигнала, для чего применяется код расширения. DSSS используется в спецификациях IEEE 802.11 и 802.11b.

D-View. Программное обеспечение SNMP компании D-Link, используемое для управления и мониторинга сетевого оборудования.

Е

EAP (англ. Extensible Authentication Protocol). Расширяемый протокол аутентификации. Протокол, поддерживающий множество механизмов аутентификации.

EIRP (англ. Effective Isotropic Radiated Power). Эквивалентная (эффективная) изотропно-излучаемая мощность. Эквивалентная мощность переданного сигнала относительно изотропного (всенаправленного) излучения. Определяется как сумма выходной мощности передатчика и коэффициента усиления антенны за вычетом потерь сигнала в кабеле и разъемах передающего тракта.

ESS (англ. Extended Service Set). Расширенный набор услуг. Два или более базовых набора услуг (BSS), соединенных распределительной системой (DS). Для подуровня LLC любой станции, ассоциированной с одним из базовых наборов услуг, расширенный набор услуг представляется единым логическим базовым набором услуг.

Ethernet. Наиболее распространенная на сегодняшний день технология локальных сетей. Описана в семействе стандартов IEEE 802.3. Используется в качестве распределительной системы в сетях 802.11.

Ф

Fading. Замирание. Изменение во времени мощности принятого сигнала, вызванное флуктуациями в среде или линии связи.

FEC (англ. Forward Error Correction). Прямое исправление ошибок. Выполняемые приемником процедуры коррекции ошибок на основании информации, содержащейся в принятом сигнале.

FHSS (англ. Frequency Hopping Spread Spectrum). Расширение спектра методом скачкообразной перестройки частоты. Разновидность технологий расширения спектра, в которой сигнал передается на разных частотах в псевдослучайной последовательности, переходя с одной частоты на другую через фиксированные промежутки времени.

FIFO (англ. First Input First Output). Тип очереди «первым пришел, первым ушел».

Fragmentation. Фрагментация. Функция подуровня MAC, выполняющая дробление исходного кадра на кадры меньшего размера (фрагменты) до его передачи.

Frame. Кадр. Единица информации на канальном уровне модели OSI. В локальной сети кадр представляет собой единицу данных подуровня MAC, содержащую управляющие данные и пакет сетевого уровня. Иногда для обозначения кадров

используется термин пакет, но термины кадр или фрейм никогда не используются для обозначения пакетов сетевого уровня. Кадр обычно содержит ограничители, управляющие поля, адреса, контрольную сумму и собственно информацию.

Frequency. Частота. Количество колебаний сигнала в секунду. Измеряется в герцах (Гц).

FSPL (англ. Free Space Path Loss). Потери в свободном пространстве. Потеря энергии сигнала, вызванная его рассеянием в пространстве.

G

GTK (англ. Group Temporal Key). Групповой временный ключ. Произвольное значение, назначаемое источником многоадресной группы для защиты отправляемых им многоадресных кадров. GTK может быть получен из группового мастер-ключа (Group Master Key, GMK).

H

Hidden station. Скрытая станция. Станция, чьи сигналы не могут быть определены второй станцией с помощью прослушивания несущей, но создающие помехи для сигналов, передаваемых между второй и третьей станциями.

HT (англ. High Throughput). Высокая производительность. Название физического уровня 802.11n.

I

IBSS (англ. Independent Basic Service Set). Независимый базовый набор услуг. Базовый набор услуг, формирующий автономную сеть, в которой отсутствует доступ к распределительной системе.

IEEE (англ. Institute of Electrical and Electronic Engineers). Институт инженеров по электротехнике и радиоэлектронике. Профессиональная организация, основанная в 1963 году для координации разработки компьютерных и коммуникационных стандартов. Институт подготовил группу стандартов 802 для локальных сетей. Членами IEEE являются ANSI и ISO.

IEEE 802.1X authentication. Аутентификация IEEE 802.1X. Аутентификация EAP, использующая в качестве транспорта протокол 802.1X.

Infrastructure. Инфраструктура. Включает среду передачи распределительной системы, точку доступа и портал. Также является логическим местоположением услуг распределения и интеграции расширенного набора услуг (ESS).

Interference. Интерференция. Взаимное увеличение или уменьшение результирующей амплитуды двух или нескольких когерентных волн при их наложении друг на друга. Существует несколько видов интерференции. Наличие интерференции является нежелательным эффектом в беспроводных сетях, поскольку приводит к уменьшению их производительности.

IP (англ. Internet Protocol). Протокол IP. Часть стека протоколов TCP/IP. Описывает программную маршрутизацию пакетов и адресацию устройств. Используется для передачи базовых блоков данных и дейтаграмм IP через сеть. Обеспечивает передачу пакетов без организации соединений и гарантии доставки. Регламентируется RFC 791 и др.

IP address. IP-адрес. Адрес для протокола IPv4 — 32-битовое (4 байта) значение, определенное в STD 5 (RFC 791) и используемое для представления точек подключения в сети TCP/IP. IP-адрес состоит из номера сети (network portion) и номера узла (host portion). Такое разделение позволяет сделать маршрутизацию более эффективной. Обычно для записи IP-адресов используют десятичную нотацию с разделением точками. Новая версия протокола IPv6 использует 128-рядные адреса, решая тем самым проблему нехватки адресного пространства.

Isotropic antenna. Изотропная антенна. Идеальная (теоретическая) антенна, излучающая электромагнитную энергию одинаковой интенсивности во всех направлениях.

L

LAN (англ. Local Area Network). Локальная сеть. Высокоскоростная компьютерная сеть, покрывающая относительно небольшую площадь. Локальные сети объединяют рабочие станции, периферийные устройства, терминалы и другие устройства, находящиеся в одном здании или на другой небольшой территории.

Latency. Задержка. Временная задержка между моментом получения устройством пакета и его отправкой на порт назначения.

Link budget. Энергетический потенциал линии связи. Разность между измеренными уровнями средней мощности излучения на выходе передающего и входе приемного устройств при вносимом затухании, обеспечивающем допустимое значение коэффициента ошибок.

LLC (англ. Logical Link Control). Управление логическим каналом. Подуровень в спецификации IEEE 802. Обеспечивает взаимодействие с сетевым уровнем и предоставляет сервисы с установлением и без установления соединения. Не зависит от метода доступа к среде передачи.

Load Balancing. Балансировка нагрузки. Распределение процесса выполнения заданий между несколькими устройствами сети с целью оптимизации использования ресурсов и сокращения времени вычисления.

M

MAC (англ. Media Access Control). Управление доступом к среде передачи. Подуровень в спецификации IEEE 802. Описывает протоколы, реализующие различные методы доступа к среде передачи, отвечает за физическую адресацию, формирование кадров и обнаружение ошибок.

MAC address. MAC-адрес. Адрес канального уровня, который требуется задавать для каждого порта или устройства, подключенного к локальной сети. Длина MAC-адреса составляет 6 байт, а их содержимое регламентируется IEEE. MAC-адреса также называют аппаратными или физическими адресами.

MCS (англ. Modulation and Coding Set). Схема модуляции и кодирования. Номер, назначаемый каждой комбинации модуляции, скорости кодирования и количества пространственных потоков в 802.11n и 802.11ac.

MIC (англ. Message Integrity Code). Код целостности сообщения. Значение, сгенерированное криптографической функцией.

MIMO (англ. Multiple Input Multiple Output). Радиоантенная технология, использующая для передачи и приема данных множество антенн и преимущества многоручевого распространения сигналов. Существует несколько форм MIMO.

Modulation. Модуляция. Процесс или результат изменения некоторых характеристик сигнала, называемого несущим, в соответствии с информационным сигналом.

MPDU (англ. MAC Protocol Data Unit). Блок данных протокола MAC. Модуль данных, которым обмениваются два одноранговых объекта MAC, используя услуги физического уровня.

MRC (англ. Maximum Ratio Combined). Метод комбинирования сигналов, полученных от множества антенн с целью повышения отношения сигнал/шум.

MSDU (англ. MAC Service Data Unit). Блок данных сервиса MAC. Информация, передаваемая единым блоком между пользователями MAC, обычно это PDU уровня LLC.

Multicast. Многоадресная рассылка. Доставка потока данных группе узлов на IP-адрес группы многоадресной рассылки.

Multicast address. Групповой адрес. Общий адрес, который относится к некоторой группе сетевых устройств.

MU-MIMO (англ. Multi-User MIMO). Многопользовательская форма MIMO. Технология, позволяющая множеству станций с одной или несколькими антеннами одновременно передавать одной станции или получать от нее независимые потоки данных в одном частотном диапазоне.

N

NAV (англ. Network Allocation Vector). Вектор сетевого распределения. Используется MAC-подуровнем 802.11 для выполнения виртуального механизма контроля несущей.

Network Address. Сетевой адрес. Адрес сетевого уровня, который относится к логическому, а не к физическому сетевому устройству. Также называется протокольным адресом (protocol address).

Node. Узел. Точка присоединения к сети, устройство, подключенное к сети.

О

OFDM (англ. Orthogonal Frequency-Division Multiplexing). Мультиплексирование с ортогональным частотным разделением. Процесс разделения полосы пропускания на множество поднесущих (subcarrier) или вспомогательных несущих. На OFDM основаны спецификации 802.11a и 802.11g, 802.11n и 802.11ac используют MIMO для передачи множества потоков OFDM.

Omni-directional antenna. Всенаправленная антенна. Антенна, излучающие свойства которой одинаковы в любой момент времени по всем азимутальным направлениям.

Р

Packet. Пакет. Группа бит, включающая данные и служебные поля, представленная в соответствующем формате и передаваемая целиком. Структура пакета зависит от протокола. В общем случае пакет включает три основных элемента: управляющую информацию (адрес получателя и отправителя, длина пакета и т. п.), передаваемые данные, биты контроля и исправления ошибок.

Passive scanning. Пассивное сканирование. Функция обнаружения точек доступа клиентами 802.11, прослушивающими каждый канал в течение определенного периода времени на предмет обнаружения передаваемых точками доступа сигнальных кадров (Beacon).

PDU (англ. Protocol Data Unit). Модуль данных протокола. Термин OSI для пакетов данных.

PMK (англ. Pairwise Master Key). Парный мастер-ключ. Ключ, сгенерированный каким-либо методом протокола EAP или полученный непосредственно из предварительно установленного ключа (PSK).

PPDU (англ. PLCP Protocol Data Unit). Модуль данных протокола PLCP. Полный кадр PLCP включает заголовок PLCP, заголовок MAC, поле данных MAC, концевики MAC и PLCP.

PoE (англ. Power over Ethernet). Технология передачи питания по кабелю на основе витой пары в сетях Ethernet. Регламентируется стандартами IEEE 802.3af и 802.3at, которые в настоящее время являются частью стандарта IEEE 802.3–2012.

Portal. Портал. Логическая точка, предоставляющая услуги интеграции.

Primary channel. Основной (первичный) канал. Общий частотный канал работы всех станций, являющихся членами одного базового набора услуг (BSS).

Protection mechanism. Механизм защиты. Любая процедура, которая до передачи кадра обновляет вектор сетевого распределения (NAV) всех станций-получателей, чей физический уровень не может правильно его интерпретировать.

PSK (англ. PreShared Key). Предварительно установленный ключ. Статический ключ, обычно распределяемый между объектами системы администратором сети вручную.

PTK (англ. Pairwise Transient Key). Парный временный ключ. Составной ключ, полученный из парного мастер-ключа (ПМК). Его компоненты включают ключ подтверждения ключа (КСК), ключ шифрования ключа (КЕК) и один или несколько временных ключей, используемых для защиты информации, передаваемой через канал связи.

PVID (англ. Port VLAN ID). Идентификатор порта VLAN.

Q

QAM (англ. Quadrature Amplitude Modulation). Квадратурная амплитудная модуляция. Метод модуляции, который для представления бит информации использует одновременно амплитудную и фазовую манипуляции.

QoS (англ. Quality of Service). Качество обслуживания. Показатель эффективности системы передачи данных, который отражает соответствие сети соглашению о передаче трафика.

QPSK (англ. Quadrature Phase Shift Keying). Квадратурная (четырёхуровневая) фазовая манипуляция. Метод модуляции, который использует четыре значения фазы несущего сигнала, каждое состояние фазы выполняет передачу сразу двух бит информации.

R

RADIUS (англ. Remote Authentication Dial-In User Service). Служба аутентификации удаленных пользователей. Протокол реализации аутентификации, авторизации и сбора сведений об использованных ресурсах, разработанный для передачи сведений между центральной платформой и канальным оборудованием. Регламентируется RFC 2865 и др.

Repeater. Повторитель. Устройство, получающее и ретранслирующее сигналы с целью расширения дальности передачи.

Redundancy. Избыточность. Дублирование устройств, сервисов и соединений. В случае неисправности позволяет избыточным устройствам, службам и соединениям выполнять функции исправных.

Reliability. Надежность. В общем случае свойство объекта сохранять во времени в установленных пределах значения всех параметров, характеризующих его способность выполнять требуемые функции в заданных режимах и условиях применения, технического обслуживания, хранения и транспортирования.

Rogue access point. Несанкционированная точка доступа. Точка доступа, которая не авторизована и настройки которой могут позволить получить несанкционированный доступ к ресурсам сети.

Router. Маршрутизатор. Устройство сетевого уровня, отвечающее за принятие решений о выборе одного из нескольких путей передачи сетевого трафика. Маршрутизаторы отправляют пакеты из одной сети в другую на основе информации сетевого уровня.

Routing. Маршрутизация. Процесс выбора оптимального маршрута передачи сообщения.

RSSI (англ. Received Signal Strength Indication). Индикатор мощности полученного сигнала. Значение, сообщающее о мощности полученного сигнала; чаще всего мощность выражается в дБм (dBm).

RSTP (англ. Rapid Spanning Tree Protocol). Протокол RSTP является развитием протокола STP. Первоначально определен в стандарте IEEE 802.1w–2001, в настоящее время определен в стандарте IEEE 802.1D–2004.

S

Secondary channel. Вторичный канал. Канал шириной 20 МГц, ассоциированный с первичным каналом, используемый станцией 802.11n для создания канала шириной 40 МГц.

SMB (англ. Small-to-Medium Business). Малые и средние предприятия. Название сегмента рынка электроники. Характеризует устройства, предназначенные для использования в сетях малых и средних предприятий с численностью сотрудников от 100 до 999 человек.

SNMP (англ. Simple Network Management Protocol). Простой протокол управления сетью. Протокол седьмого уровня модели OSI, разработанный для управления и мониторинга сетевыми устройствами. Протокол SNMP позволяет получать информацию о состоянии устройств сети, обнаруживать и исправлять неисправности и планировать развитие сети. Регламентируется RFC 1157, 1901–1908, 3411–3418 и др.

SNR (англ. Signal-to-Noise Ratio). Отношение сигнал/шум. Значение, определяемое как отношение мощности сигнала к мощности шума (помех) и выражаемое в децибелах (дБ, dB).

SOHO (англ. Small Office, Home Office). Малый/домашний офис. Название сегмента рынка электроники. Как правило, характеризует устройства, предназначенные для домашнего использования или использования в небольших офисах и не рассчитанные на производственные нагрузки.

Spatial multiplexing. Пространственное мультиплексирование. Метод передачи, при котором потоки данных передаются через множество пространственных каналов, создающихся множеством передающих и приемных антенн.

Spatial stream. Пространственный поток. Один из нескольких потоков бит или символов модуляции, передающихся через множество пространственных измерений, создаваемых множеством антенн на обоих концах линии связи.

Spread spectrum. Расширенный спектр. Метод распространения информации по расширенной полосе частот с использованием кода расширения.

Spectrum. Спектр. Понятие, означающее абсолютный диапазон частот.

SSH (англ. Secure Shell). Безопасная оболочка. Сетевой протокол сеансового уровня, позволяющий осуществлять удаленное управление операционной системой устройств (серверов, сетевого оборудования). Регламентируется RFC 4253 и др.

SSID (англ. Service Set Identifier). Идентификатор набора услуг. Текстовая строка длиной до 32 байт, используемая для идентификации определенной беспроводной сети.

SSL (англ. Secure Sockets Layer). Уровень защищенных сокетов. Криптографический протокол, обеспечивающий безопасную передачу данных по сети Интернет. Регламентируется RFC 2246, 4346 и др.

STBC (англ. Space-Time Block Coding). Пространственно-временное блочное кодирование. Метод передачи одного потока данных через множество антенн с целью обеспечения надежности передачи.

STP (англ. Spanning Tree Protocol). Протокол связующего дерева. Описывается стандартом IEEE 802.1D—2004. Использует алгоритм связующего дерева. Позволяет самообучающемуся мосту динамически обрабатывать коммутационные петли в сетевой топологии путем создания связующего дерева. Мосты обнаруживают петли путем обмена сообщениями BPDU с другими мостами и ликвидируют петли посредством блокирования выбранных мостовых интерфейсов.

Switch. Коммутатор. Сетевое устройство, которое фильтрует, пересылает и направляет кадры в зависимости от их адреса приемника. Коммутатор, работающий на канальном уровне модели OSI, называется L2-коммутатором. Коммутатор, работающий на канальном и сетевом уровнях модели OSI, называется L3-коммутатором, он выполняет коммутацию кадров и маршрутизацию пакетов между различными подсетями или виртуальными локальными сетями.

Т

Tag. Тег. Идентификационная информация, в том числе и номер.

TCP (англ. Transmission Control Protocol). Протокол управления передачей. Ориентированный на соединение протокол транспортного уровня, обеспечивающий надежную дуплексную передачу данных. TCP входит в стек протоколов TCP/IP. Регламентируется RFC 675, 793, 2581 и др.

Temporal encryption key. Временный ключ шифрования. Часть парного временного ключа (РТК) или группового временного ключа (GTK), используемая для шифрования данных в блоках данных протокола MAC (MPDU).

Temporal key. Временный ключ. Комбинация временного ключа шифрования и временного ключа кода целостности сообщения (MIC).

Temporal message integrity code (MIC) key. Временный ключ кода целостности сообщения. Часть временного ключа, используемая для гарантии целостности блоков данных сервиса MAC (MSDU) или блоков данных протокола MAC (MPDU).

Throughput. Пропускная способность. Максимально возможная скорость передачи информации через канал, определенная его ограничениями. Измеряется в битах в секунду (бит/с или bps — bits per second) и производных единицах.

TKIP (англ. Temporal Key Integrity Protocol). Протокол целостности временного ключа. Является частью стандарта IEEE 802.11i. TKIP использует основные операции WEP, но усиливает его криптографическую стойкость благодаря добавлению сервисов целостности сообщений и конфиденциальности данных.

ToS (англ. Type of Service). Тип сервиса. Поле в заголовке протокола IP, используемое для обеспечения QoS.

TPID (англ. Tag Protocol Identifier). Идентификатор протокола тегирования в кадрах протоколов IEEE 802.1Q и IEEE 802.1ad.

Trunk. Магистраль. Физическое и логическое соединение между двумя коммутаторами, по которому передается сетевой трафик.

U

UDP (англ. User Datagram Protocol). Протокол дейтаграмм пользователя. Протокол транспортного уровня, не требующий подтверждения соединения. Входит в стек протоколов TCP/IP. UDP обеспечивает обмен дейтаграммами без подтверждения и гарантий доставки.

Unified Access Point. Унифицированная точка доступа. Точка доступа, которая может управляться как независимо от других, так и централизованно с помощью беспроводного контроллера.

V

VHT (англ. Very High Throughput). Очень высокая производительность. Название физического уровня 802.11ac.

VID (VLAN ID). Идентификатор VLAN.

VoIP (англ. Voice over IP). IP-телефония. Система связи, обеспечивающая передачу речевого сигнала по IP-сетям.

VLAN (англ. Virtual LAN). Виртуальная локальная сеть. Группа устройств, принадлежащих одной или нескольким локальным сетям и сконфигурированных при помощи программного обеспечения таким образом, что обмен данными между ними происходит так, как будто они подключены к одному коммутатору, хотя на самом деле они находятся в разных сегментах локальной сети. VLAN строятся на основе логических соединений.

VPN (англ. Virtual Private Network). Виртуальные локальные сети. Различные технологии, позволяющие создавать логические сети, использующие в качестве транспорта другие сетевые протоколы. При этом характеристики безопасности созданной логической сети могут отличаться от характеристик безопасности транспортной сети.

W

WDS (англ. Wireless Distribution System). Беспроводная распределительная система. Термин, описывающий механизм соединения non mesh-станций, поддерживающих формат кадра с четырьмя полями адреса.

WEP (англ. Wired Equivalent Privacy). Механизм безопасности беспроводных сетей, добавлен в стандарт IEEE 802.11 в 1999 году для обеспечения конфиденциальности и целостности данных, аналогичных проводным сетям («Wired Equivalent Privacy» переводится как «конфиденциальность беспроводного эквивалента»).

Wi-Fi (англ. Wireless Fidelity). Торговая марка консорциума Wi-Fi Alliance, используется для обозначения беспроводных локальных сетей (WLAN), соответствующих стандарту IEEE 802.11.

Wi-Fi Alliance. Объединение крупнейших производителей компьютерной техники и беспроводных устройств Wi-Fi. Одной из задач альянса является тестирование оборудования различных производителей на предмет совместимости и корректности работы устройств друг с другом.

Wi-Fi CERTIFIED. Торговая марка консорциума Wi-Fi Alliance, используемая для уведомления о полном соответствии оборудования всем предъявляемым Wi-Fi Alliance требованиям к совместимости с оборудованием других производителей такой же спецификации.

WLAN (англ. Wireless LAN). Беспроводная локальная сеть. Локальная сеть, построенная на основе беспроводных технологий. При таком способе построения сетей передача данных осуществляется через радиоканалы; объединение устройств в сеть происходит без использования кабельных соединений.

WPA/WPA2 (англ. Wi-Fi Protected Access). Программы сертификации Wi-Fi Alliance, определяющие требования к безопасности беспроводных сетей. WPA основана на проекте стандарта IEEE 802.11i и включает поддержку протокола шифрования TKIP, аутентификации на основе протокола IEEE 802.1X с EAP и на основе PSK. WPA2 основана на ратифицированной версии стандарта IEEE 802.11i, включает поддержку протокола шифрования CCMP, аутентификации на основе протокола IEEE 802.1X с EAP и на основе PSK.

Y

Yagi antenna. Антенна Яги. Специализированная направленная антенна, состоящая из расположенных вдоль линии излучения параллельно друг другу активного и нескольких пассивных вибраторов.

Учебное издание

Компьютерные системы и сети

Смирнова Елена Викторовна
Пролетарский Андрей Викторович
Ромашкина Екатерина Александровна
Балюк Сергей Александрович
Суровов Александр Михайлович

Технологии современных беспроводных сетей Wi-Fi

Оригинал-макет подготовлен
в Издательстве МГТУ им. Н.Э. Баумана.

В оформлении использованы шрифты
Студии Артемия Лебедева.

Подписано в печать 22.11.2016. Формат 70×100/16.
Усл. печ. л. 36,4. Тираж 700 экз. Заказ

Издательство МГТУ им. Н.Э. Баумана.
105005, Москва, 2-я Бауманская ул., д. 5, стр. 1.
press@bmstu.ru
www.baumanpress.ru

Отпечатано в АО «Областная типография «Печатный двор»
432049, г. Ульяновск, ул. Пушкарёва, 27