

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. Сюзев, 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

Компьютерные системы и сети

Выпуск 2

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»



BAUMANPRESS
МОСКВА
ИЗДАТЕЛЬСТВО
МГТУ им. Н.Э. БАУМАНА
2017

УДК 004.7
ББК 32.973.202
Т38

Авторы:
Е.В. Смирнова, А.В. Пролетарский, Е.А. Ромашкина,
С.А. Балюк, А.М. Суровов

Рецензенты:
генеральный директор АО «РтСофт», д-р техн. наук *О.В. Синенко*;
директор фирмы «1С», канд. экон. наук *Б.Г. Нуралиев*

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

Основы беспроводных сетей Wi-Fi

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 существования 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 существования 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. Развёртывание 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

Оглавление

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
Лабораторная работа № 1. Преобразование единиц измерения в беспроводных сетях	317
Лабораторная работа № 2. Создание беспроводной сети в инфраструктурном режиме	320
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
Лабораторная работа № 3. Объединение инфраструктурных BSS с единым SSID через распределительную систему	338
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
Лабораторная работа № 4. Исследование кадров MAC стандарта IEEE 802.11	342
4.1. Захват трафика с помощью сетевого анализатора Microsoft Network Monitor	345
4.2. Анализ кадров MAC стандарта IEEE 802.11	350
Лабораторная работа № 5. Изучение пассивного и активного сканирования	358
Лабораторная работа № 6. Обеспечение безопасности в беспроводных сетях	362
6.1. Настройка режима WPA/WPA2-Personal	363
6.2. Контроль доступа к беспроводной сети на основе MAC-адресов	367
Лабораторная работа № 7. Расчет беспроводной линии связи	369
7.1. Примеры расчета беспроводной линии связи	372
7.2. Задания для самостоятельного выполнения	375
Лабораторная работа № 8. Влияние скорости передачи на производительность и дальность действия сети	376
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
Лабораторная работа № 9. Настройка распределенной сети (WDS)	383
9.1. Настройка WDS-соединения типа «точка—точка»	384
9.2. Настройка WDS-соединения типа «точка—много точек»	388
Лабораторная работа № 10. Настройка сегментации сети	392
10.1. Настройка сегментации проводной и беспроводной сети	393
10.2. Настройка сегментации распределенной сети	403
Лабораторная работа № 11. Настройка функции AP Array	408
Лабораторная работа № 12. Сегментация беспроводной сети на основе двухдиапазонных точек доступа	415
Лабораторная работа № 13. Настройка программного контроллера CWM-100	423
Литература	433
Гlossарий	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, быстро-растущим 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.

Предисловие

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 слово-сочетания *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;

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).

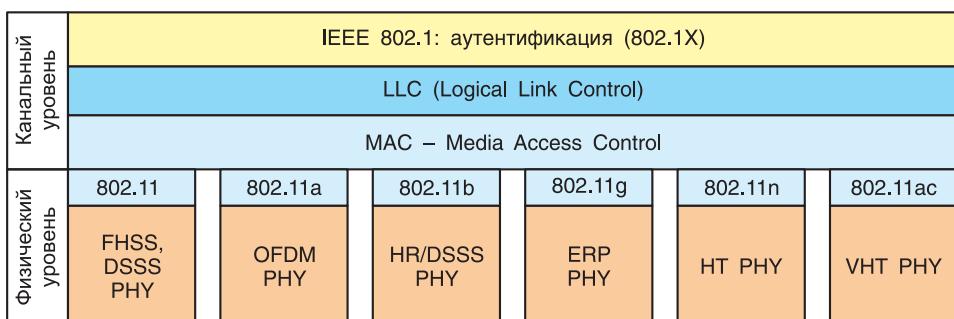


Рис. 2.1. Стек протоколов IEEE 802.11

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 состязающихся 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

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-

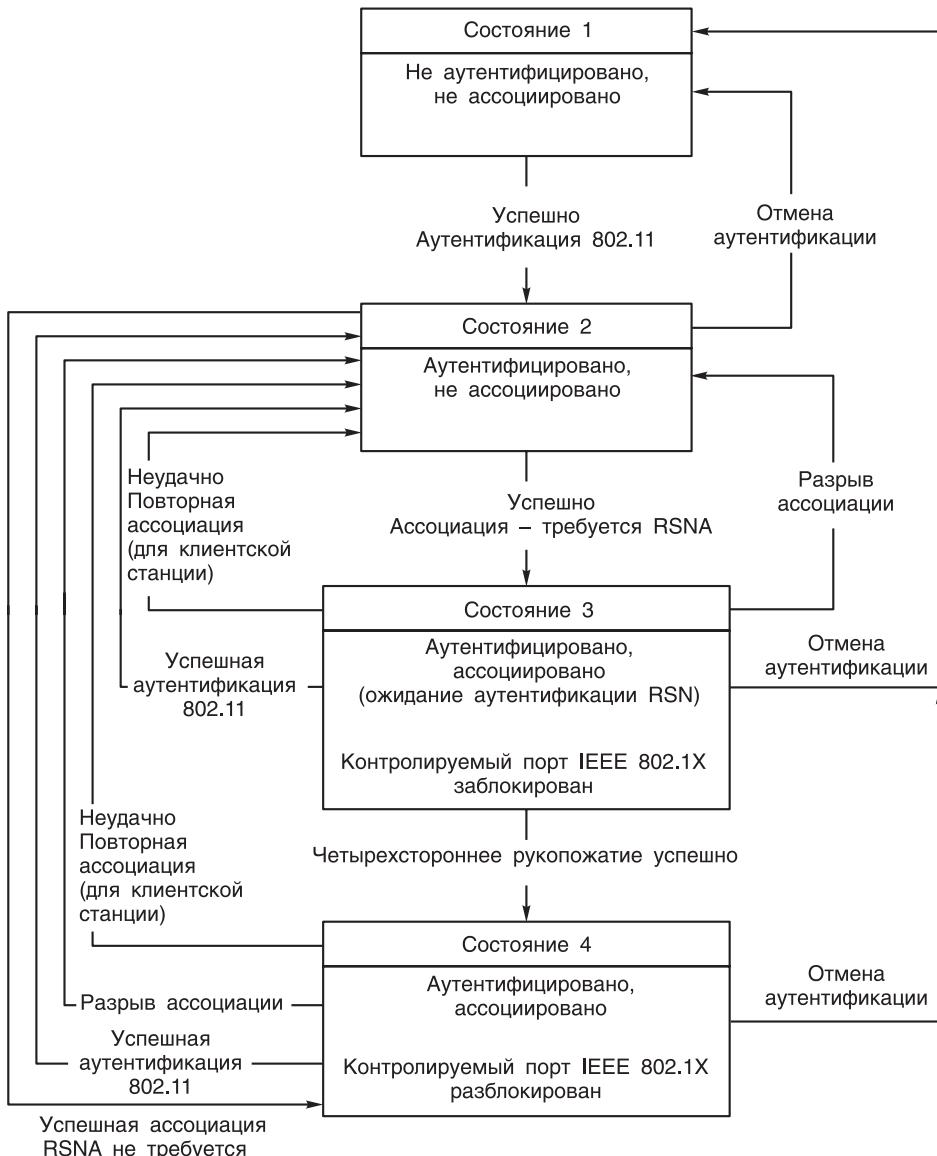


Рис. 3.1. Диаграмма состояний (машина состояний) беспроводного клиента

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

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

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

Рис. 5.1. Архитектура физического уровня 802.11

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 комплементарным 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).

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 негибают 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 antennном кабеле и разъемах передающего тракта;

- потери при распространении;
- чувствительность приемника, потери в antennом кабеле и коэффициент усиления антенны приемника.

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 компаний, 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 технологий *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

8. Развортывание беспроводной сети

Архитектура беспроводной сети согласно стандарту 802.11 может рассматриваться как тип архитектуры на основе ячеек (сот), в которой каждой ячейкой (сотовой) 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-

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) — дольная единица, равная 0,1 Б; логарифмическая единица (т. е. безразмерная относительная величина), предназначенная для измерения отношения двух одинаковых величин (например, уровней мощности, затухания и усиления сигналов) с применением к полученному отношению логарифмического масштаба. В децибелях 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

$$P_{dB} = 10 \lg \frac{P_1}{P_0}, \quad (\text{Л1.1})$$

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:

$$P_{dBm} = 10 \lg \frac{P_{mW}}{1mW}, \quad (\text{Л1.2})$$

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

Литература

1. IEEE Std 802.11TM—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 802.11acTM—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 MultimediaTechnical 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

A

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 широковещательные 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 адAPTERы.

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.

B

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 состязающихся 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 равнopravno подключаются к общей среде передачи.

C

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, пересыпает 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 двухуровневая 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. Антenna 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-

Технологии современных беспроводных сетей Wi-Fi

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.

E

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.

F

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-разрядные 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). Радиоантенна технология, использующая для передачи и приема данных множество антенн и преимущества многолучевого 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 антennами 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.

O

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. Антенны, излучающие свойства которой одинаковы в любой момент времени по всем азимутальным направлениям.

P

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 (PMK). 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 (четырехуровневая) 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 dBm (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 (dB, 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 изменений, 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, пересыпает 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 временно-го ключа (PTK) 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).

Технологии современных беспроводных сетей Wi-Fi

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 антenna, 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. Пушкинёва, 27