Лекция 1. Беспроводные технологии.

Беспроводные технологии — подкласс информационных технологий, служат для передачи информации на расстояние между двумя и более точками, не требуя связи их проводами. Для передачи информации может использоваться инфракрасное излучение, радиоволны, оптическое или лазерное излучение.

В настоящее время существует множество беспроводных технологий, наиболее часто известных пользователям по их маркетинговым названиям, таким как Wi-Fi, WiMAX, Bluetooth. Каждая технология обладает определёнными характеристиками, которые определяют её область применения.

Существуют различные подходы к классификации беспроводных технологий.

По дальности действия:

- Беспроводные персональные сети (WPAN — Wireless Personal Area Networks). Примеры технологий — Bluetooth.
- Беспроводные локальные сети (WLAN — Wireless Local Area Networks). Примеры технологий — Wi-Fi.
- Беспроводные сети масштаба города (WMAN — Wireless Metropolitan Area Networks). Примеры технологий — WiMAX.
- Беспроводные глобальные сети (WWAN — Wireless Wide Area Network). Примеры технологий — CSD, GPRS, EDGE, EV-DO, HSPA.

По топологии:

- «Точка-точка».
- «Точка-многоточка».

По области применения:

- Корпоративные (ведомственные) беспроводные сети — создаваемые компаниями для собственных нужд.
- Операторские беспроводные сети — создаваемые операторами связи для возмездного оказания услуг.

По мобильности:

- Не обеспечивается. Примеры технологий — Wi-Fi.
- Может быть обеспечена. Примеры технологий — WiMAX.

По

IEEE 802.15

Bluetooth или блютус (/bluːtuːθ/, переводится как синий зуб, или синезубый, назван в честь Харальда I Синезубого[2][3]) — производственная спецификация беспроводных персональных сетей (англ. Wireless personal area network, WPAN). Bluetooth обеспечивает обмен информацией между такими устройствами как персональные компьютеры (настольные, карманные, ноутбуки), мобильные телефоны, принтеры, цифровые фотоаппараты, мышки, клавиатуры, джойстики,

наушники, гарнитуры на надёжной, бесплатной, повсеместно доступной радиочастоте для ближней связи.

Bluetooth позволяет этим устройствам сообщаться, когда они находятся в радиусе до 100 метров друг от друга (дальность сильно зависит от преград и помех), даже в разных помещениях.

IEEE 802.15.4. ZigBee и IEEE 802.15.4

ZigBee — спецификация сетевых протоколов верхнего уровня (уровня приложений API и сетевого уровня NWK), использующих сервисы нижних уровней — уровня управления доступом к среде MAC и физического уровня PHY, регламентированных стандартом IEEE 802.15.4. ZigBee и IEEE 802.15.4 описывают беспроводные персональные вычислительные сети (WPAN). Спецификация ZigBee ориентирована на приложения, требующие гарантированной безопасной передачи данных при относительно небольших скоростях и возможности длительной работы сетевых устройств от автономных источников питания (батарей).

Модуль ZigBee (слева) и монета в 1 евро (справа) диаметром в 23 мм для сравнения размеров.

Основная особенность технологии ZigBee заключается в том, что она при малом энергопотреблении поддерживает не только простые топологии сети («точка-точка», «дерево» и «звезда»), но и самоорганизующуюся и самовосстанавливающуюся ячеистую (mesh) топологию с ретрансляцией и маршрутизацией сообщений. Кроме того, спецификация ZigBee содержит возможность выбора алгоритма маршрутизации, в зависимости от требований приложения и состояния сети, механизм стандартизации приложений — профили приложений, библиотека стандартных кластеров, конечные точки, привязки, гибкий механизм безопасности, а также обеспечивает простоту развертывания, обслуживания и модернизации. Применение сетей ZigBee в Российской Федерации в частотном диапазоне 2,405-2,485 ГГц не требует получения частотных разрешений и дополнительных согласований (Решение ГКРЧ при Мининформсвязи

России от 07.05.2007 № 07-20-03-001).

IEEE 802.11

IEEE 802.11 — набор стандартов связи для коммуникации в беспроводной локальной сетевой зоне частотных диапазонов 0,9; 2,4; 3,6 и 5 Ггц.

Пропускная способность от 10 Мбит/сек до 600 Мбит/сек.

Пользователям более известен по названию Wi-Fi, фактически являющемуся брендом, предложенным и продвигаемым организацией Wi-Fi Alliance. Получил широкое распространение благодаря развитию в мобильных электронно-вычислительных устройствах: КПК и ноутбуках.

Изначально стандарт IEEE 802.11 предполагал возможность передачи данных по радиоканалу на скорости не более 1 Мбит/с и опционально на скорости 2 Мбит/с. Один из первых высокоскоростных стандартов беспроводных сетей — IEEE 802.11a — определяет скорость передачи уже до 54 Мбит/с. Рабочий диапазон стандарта - 5 ГГц.

Вопреки своему названию, принятый в 1999 году стандарт IEEE 802.11b не является продолжением стандарта 802.11a, поскольку в них используются различные технологии: DSSS (точнее, его улучшенная версия HR-DSSS) в 802.11b против OFDM в 802.11a. Стандарт предусматривает использование нелицензируемого диапазона частот 2,4 ГГц. Скорость передачи до 11 Мбит/с.

Продукты стандарта IEEE 802.11b, поставляемые разными изготовителями, тестируются на совместимость и сертифицируются организацией Wireless Ethernet Compatibility Alliance (WECA), которая в настоящее время больше известна под названием Wi-Fi Alliance. Совместимые беспроводные продукты, прошедшие

испытания по программе «Альянса Wi-Fi», могут быть маркированы знаком Wi-Fi.

Долгое время IEEE 802.11b был распространённым стандартом, на базе которого было построено большинство беспроводных локальных сетей. Сейчас его место занял стандарт IEEE 802.11g, постепенно вытесняемый высокоскоростным IEEE 802.11n.

Проект стандарта IEEE 802.11g был утверждён в октябре 2002 г. Этот стандарт предусматривает использование диапазона частот 2,4 ГГц, обеспечивая скорость соединения до 54 Мбит/с и превосходя, таким образом, стандарт IEEE 802.11b, который обеспечивает скорость соединения до 11 Мбит/с. Кроме того, он гарантирует обратную совместимость со стандартом 802.11b. Обратная совместимость стандарта IEEE 802.11g может быть реализована в режиме модуляции DSSS, и тогда скорость соединения будет ограничена одиннадцатью мегабитами в секунду либо в режиме модуляции OFDM, при котором скорость может достигать 54 Мбит/с. Таким образом, данный стандарт является наиболее приемлемым при построении беспроводных сетей.

Стандарт 802.11n повышает скорость передачи данных практически вчетверо по сравнению с устройствами стандартов 802.11g (максимальная скорость которых равна 54 Мбит/с), при условии использования в режиме 802.11n с другими устройствами 802.11n. Теоретически 802.11n способен обеспечить скорость передачи данных до 600 Мбит/с, применяя передачу данных сразу по четырём антеннам. По одной антенне — до 150 Мбит/с.

Устройства 802.11n работают в диапазонах 2,4—2,5 или 5,0 Ггц.

IEEE 802.16

WiMAX (англ. Worldwide Interoperability for Microwave Access) — телекоммуникационная технология, разработанная с целью предоставления универсальной беспроводной связи на больших расстояниях для широкого спектра устройств (от рабочих станций и портативных компьютеров до мобильных телефонов). Основана на стандарте IEEE 802.16, который также называют Wireless MAN (WiMAX следует считать жаргонным названием, так как это не технология, а название форума, на котором Wireless MAN и был согласован).

Название «WiMAX» было создано WiMAX Forum — организацией, которая была основана в июне 2001 года с целью продвижения и развития технологии WiMAX. Форум описывает WiMAX как «основанную на стандарте технологию, предоставляющую высокоскоростной беспроводной доступ к сети, альтернативный выделенным линиям и DSL». Максимальная скорость — до 1 Гбит/сек на ячейку.

Поколения мобильной телефонии

Поколение	1G	2G	2,5G	3G	3,5G	4G
Начало разработок	1970	1980	1985	1990	<2000	2000
Реализация	1984	1991	1999	2002	2006-2007	2008-2010
Сервисы	аналоговый стандарт, речевые сообщения	цифровой стандарт, поддержка коротких сообщений (SMS), передача данных со скоростью до 9,6 кбит/с	большая ёмкость, пакетная передача данных, увеличение скорости сетей второго поколения	ещё большая ёмкость, скорости до 2 Мбит/с	увеличение скорости сетей третьего поколения	большая ёмкость, IP-ориентированная сеть, поддержка мультимедиа, скорости до сотен мегабит в секунду
Скорость передачи	1,9 кбит/с	9,6-14,4 кбит/с	115 кбит/с (1 фаза), 384 кбит/с (2 фаза)	2 Мбит/с	3-14 Мбит/с	100 Мбит/с - 1 Гбит/с
Стандарты	AMPS, TACS, NMT	TDMA, CDMA, GSM, PDC	GPRS, EDGE (2.75G), 1xRTT	WCDMA, CDMA2000, UMTS	HSDPA, HSUPA, HSPA, HSPA+	LTE-Advanced, WiMax Release 2 (IEEE

						802.16m), WirelessMAN-Advanced
Сеть	PSTN	PSTN	PSTN, сеть пакетной передачи данных	сеть пакетной передачи данных	сеть пакетной передачи данных	сеть пакетной передачи данных

1G

Все первые системы сотовой связи были аналоговыми. К ним относятся:

AMPS (Advanced Mobile Phone Service — усовершенствованная мобильная телефонная служба, диапазон 800 МГц) — широко используется в США, Канаде, Центральной и Южной Америке, Австралии; известен также как «североамериканский стандарт»; это наиболее распространённый стандарт в мире, обслуживающий почти половину всех абонентов сотовой связи (вместе с цифровой модификацией D-AMPS, речь о которой впереди); использовался в России в качестве регионального стандарта (в основном — в варианте D-AMPS), где он также являлся наиболее распространённым; На данный момент морально устарел. 18 апреля 2008 года прекратила свою работу двустандартная сеть AMPS/CDMA-800 Fora Commmunications (принадлежала Теле2) в Санкт-Петербурге — последняя крупная сеть стандарта AMPS.

TACS (Total Access Communications System — общедоступная система связи, диапазон 900 МГц) — используется в Англии, Италии, Испании, Австрии, Ирландии, с модификациями ETACS (Англия) и JTACS/NTACS (Япония); это второй по распространённости стандарт среди аналоговых; ещё недавно, в 1995 г., он занимал и общее второе место в мире по величине абонентской базы, но в 1997 г. оттеснён на четвёртое место более быстро развивающимися цифровыми стандартами;

NMT-450 и NMT 900 (Nordic Mobile Telephone — мобильный телефон северных стран, диапазоны 450 и 900 МГц соответственно) — используется в Скандинавии и во многих других странах; известен также как «скандинавский стандарт»; третий по распространённости среди аналоговых стандартов мира; стандарт NMT 450 является одним из двух стандартов сотовой связи, принятых в России в качестве федеральных (второй — цифровой стандарт GSM 900);

C-450 (диапазон 450 МГц) — используется в Германии и Португалии;

RTMS (Radio Telephone Mobile System — мобильная радиотелефонная система, диапазон 450 МГц) — используется в Италии;

Radiocom 2000 (диапазоны 170, 200, 400 МГц) — используется во Франции;

NTT (Nippon Telephone and Telegraph system — японская система телефона и телеграфа, диапазон 800…900 МГц — в трех вариантах) — используется в Японии.

Во всех аналоговых стандартах применяются частотная модуляция для передачи речи и частотная манипуляция для передачи информации управления (или сигнализации — signaling). Этим так же была обусловлена интерференция сигнала. Как правило подвижная станция первого поколения имела высокую мощность(3-5 Вт). Для передачи информации различных каналов используются различные участки спектра частот — применяется метод множественного доступа с частотным разделением каналов (Frequency Division Multiple Access — FDMA), с полосами каналов в различных стандартах от 12,5 до 30 кГц. С этим непосредственно связан основной недостаток аналоговых систем — относительно низкая ёмкость, являющаяся прямым следствием недостаточно рационального использования выделенной полосы частот при частотном разделении каналов. Этот недостаток стал очевиден уже к середине 80-х годов, в самом начале широкого распространения сотовой связи в ведущих странах, и сразу же значительные силы были направлены на поиск более совершенных технических решений. В результате этих усилий и поисков появились цифровые сотовые системы второго поколения. Переход к цифровым системам сотовой связи стимулировался также широким внедрением цифровой техники в связь в целом и

в значительной степени был обеспечен разработкой низкоскоростных методов кодирования и появлением сверхминиатюрных интегральных схем для цифровой обработки сигналов.

2G

В США аналоговый стандарт AMPS получил столь широкое распространение, что прямая замена его цифровым оказалась практически невозможной. Выход был найден в разработке двухрежимной аналого-цифровой системы, позволяющей совмещать работу аналоговой и цифровой систем в одном и том же диапазоне. Работа над соответствующим стандартом была начата в 1988 г. и закончена в 1992 г.; стандарт получил наименование D-AMPS, или IS-54 (IS — сокращение от Interim Standard, то есть «промежуточный стандарт»). Его практическое использование началось в 1993 г. В Европе ситуация осложнялась наличием множества несовместимых аналоговых систем («лоскутное одеяло»). Здесь выходом оказалась разработка единого общеевропейского стандарта GSM (GSM 900 — диапазон 900 МГц). Соответствующая работа была начата в 1982, г., к 1987 г. были определены все основные характеристики системы, а в 1988 г. приняты основные документы стандарта. Практическое применение стандарта началось с 1991 г. Еще один вариант цифрового стандарта, по техническим характеристикам схожий с D-AMPS, был разработан в Японии в 1993 г.; первоначально он назывался JDC, а с 1994 г. — PDC (Personal Digital Cellular — буквально «персональная цифровая сотовая связь»). Но на этом развитие цифровых систем сотовой связи не остановилось.

Стандарт D-AMPS дополнительно усовершенствовался за счёт введения нового типа каналов управления. Дело в том, что цифровая версия IS-54 сохранила структуру каналов управления аналогового AMPS, что ограничивало возможности системы. Новые чисто цифровые каналы управления введены в версии IS-136, которая была разработана в 1994 г. и начала применяться в 1996 г. При этом была сохранена совместимость с AMPS и IS-54, но повышена ёмкость канала управления

и заметно расширены функциональные возможности системы. Стандарт GSM, продолжая совершенствоваться технически (последовательно вводимые фазы 1, 2 и 2+), в 1989 г. пошёл на освоение нового частотного диапазона 1800 МГц. Это направление известно под названием системы персональной связи. Отличие последней от исходной системы GSM 900 не столько техническое, сколько маркетинговое при технической поддержке: более широкая рабочая полоса частот в сочетании с меньшими размерами ячеек (сот) позволяет строить сотовые сети значительно большей ёмкости, и именно расчёт на массовую систему мобильной связи с относительно компактными, лёгкими, удобными и недорогими абонентскими терминалами был заложен в основу этой системы. Соответствующий стандарт (в виде дополнений к исходному стандарту GSM 900) был разработан в Европе в 1990—1991 гг. Система получила название DCS 1800 (Digital Cellular System — цифровая система сотовой связи; первоначально использовалось также наименование PCN — Personal Communications Network, что в буквальном переводе означает «сеть персональной связи») и начала использоваться с 1993 г. В 1996 г. было принято решение именовать её GSM 1800. В США диапазон 1800 МГц оказался занят другими пользователями, но была найдена возможность выделить полосу частот в диапазоне 1900 МГц, которая получила в Америке название диапазона систем персональной связи (PCS — Personal Communications Systems), в отличие от диапазона 800 МГц, за которым сохранено название сотового (cellular). Освоение диапазона 1900 МГц началось с конца 1995 г.; работа в этом диапазоне предусмотрена стандартом D-AMPS (версия IS-136, но аналогового AMPS в диапазоне 1900 МГц уже нет), и разработана соответствующая версия стандарта GSM («американский» GSM 1900 — стандарт IS-661).

2.5G

GPRS (англ. General Packet Radio Service — пакетная радиосвязь общего пользования) — надстройка над технологией мобильной связи GSM, осуществляющая пакетную передачу данных. GPRS позволяет пользователю мобильного телефона производить обмен данными с другими устройствами в сети GSM и с внешними сетями, в том числе Интернет. GPRS предполагает

тарификацию по объёму переданной/полученной информации, а не времени.

XRTT (One Times Radio Transmission Technology) — 2.5G мобильная технология передачи цифровых данных основанная на CDMA-технологии. Использует принцип передачи с коммутацией пакетов. Теоретически возможная скорость передачи 144 Кбит/сек, но на практике реальная скорость менее 40-60 Кбит/сек. 1XRTT использует лицензируемый радиочастотный диапазон и, подобно другим мобильным технологиям, широко распространена.

2.75G

EDGE (англ. Enhanced Data rates for GSM Evolution) — цифровая технология для мобильной связи, которая функционирует как надстройка над 2G и 2.5G (GPRS) сетями. Эта технология работает в TDMA и GSM сетях. Для поддержки EDGE в сети GSM требуются определённые модификации и усовершенствования. На основе EDGE могут работать: ECSD — ускоренный доступ в Интернет по каналу CSD, EHSCSD — по каналу HSCSD, и EGPRS — по каналу GPRS. EDGE был впервые представлен в 2003 году в Северной Америке.

3G

Все перечисленные выше цифровые системы второго поколения основаны на методе множественного доступа с временным разделением каналов (Time Division Multiple Access — TDMA). Однако уже в 1992—1993 гг. в США был разработан стандарт системы сотовой связи на основе метода множественного доступа с кодовым разделением каналов (Code Division Multiple Access — CDMA) — стандарт IS-95 (диапазон 800 МГц). Он начал применяться с 1995−1996 гг. в Гонконге, США, Южной Корее, причём в Южной Корее -наиболее широко, а в США начала использоваться и версия этого стандарта для диапазона 1900 МГц. Направление персональной связи нашло своё преломление и в Японии, где в 1991—1992 гг. была разработана и с 1995 г. начала широко использоваться система PHS диапазона 1800 МГц (Personal Handyphone System — буквально

«система персонального ручного телефона»).

3.5G

HSDPA (англ. High-Speed Downlink Packet Access — высокоскоростная пакетная передача данных от базовой станции к мобильному телефону) — стандарт мобильной связи, рассматривается специалистами как один из переходных этапов миграции к технологиям мобильной связи четвёртого поколения (4G). Максимальная теоретическая скорость передачи данных по стандарту составляет 14,4 Мбит/сек., практическая достижимая в существующих сетях — около 8 Мбит/сек.

4G

Технологии, претендующие на роль 4G (и очень часто упоминаемые в прессе в качестве 4G):

- LTE
- TD-LTE
- Mobile WiMAX
- UMB

В настоящее время запущены сети WiMAX и LTE. Первую в мире сеть LTE в Стокгольме и Осло запустил альянс TeliaSonera/Ericsson — расчётное значение максимальной скорости передачи данных к абоненту составляет 382 Mbps и 86 Mbps — от абонента. Насчёт UMB планы внедрения не известны, так как ни один оператор (в мировом масштабе) не заключил контракт на его тестирование. Стоит отметить, что стандарт WiMAX не все относят к 4G, так как он не интегрирован с сетями предыдущих поколений таких как 3G и 2G, а также из-за того, что в сети WiMAX сами операторы не предоставляют традиционные услуги связи, такие как

голосовые звонки и SMS, хотя и пользование ими возможно при использовании различных VoIP сервисов. IMT разрешил сетям HSPA+ называться 4G, т.к. они обеспечивают соответствующие скорости.

Лекция 2. Методы доступа в беспроводных сетях

Технология расширенного спектра

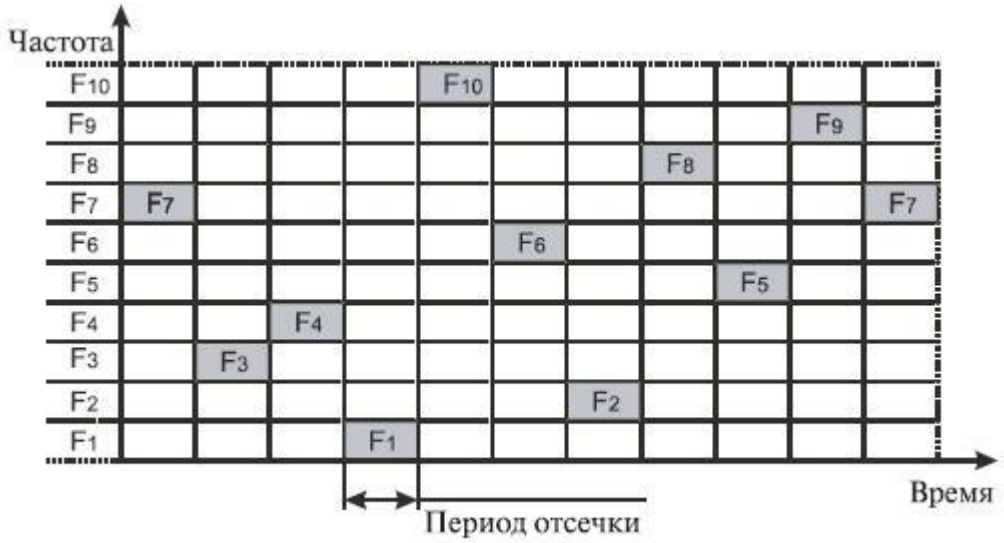
Изначально метод расширенного спектра создавался для разведывательных и военных целей. Основная идея метода состоит в том, чтобы распределить информационный сигнал по широкой полосе радиодиапазона, что в итоге позволит значительно усложнить подавление или перехват сигнала. Первая разработанная схема расширенного спектра известна как метод перестройки частоты. Более современной схемой расширенного спектра является метод прямого последовательного расширения. Оба метода используются в различных стандартах и продуктах беспроводной связи.

Расширение спектра скачкообразной перестройкой частоты (Frequency Hopping Spread Spectrum - FHSS)

Для того чтобы радиообмен нельзя было перехватить или подавить узкополосным шумом, было предложено вести передачу с постоянной сменой несущей в пределах широкого диапазона частот. В результате мощность сигнала распределялась по всему диапазону, и прослушивание какой-то определенной частоты давало только небольшой шум. Последовательность несущих частот была псевдослучайной, известной только передатчику и приемнику. Попытка подавления сигнала в каком-то узком диапазоне также не слишком ухудшала сигнал, так как подавлялась только небольшая часть информации.

Идею этого метода иллюстрирует рисунок.

В течение фиксированного интервала времени передача ведется на неизменной несущей частоте.

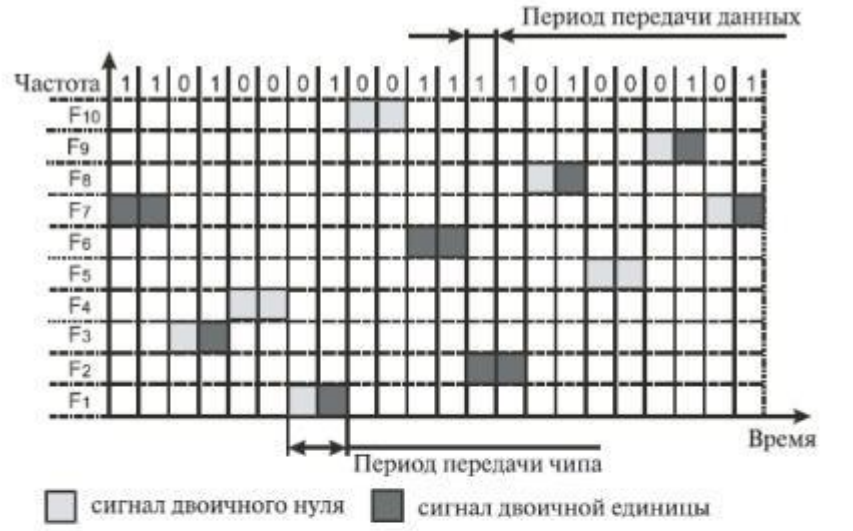


Последовательность перестройки частот: F_7-F_3-F_4-F_1-F_{10}-F_6-F_2-F_8-F_5-F_9-F_7

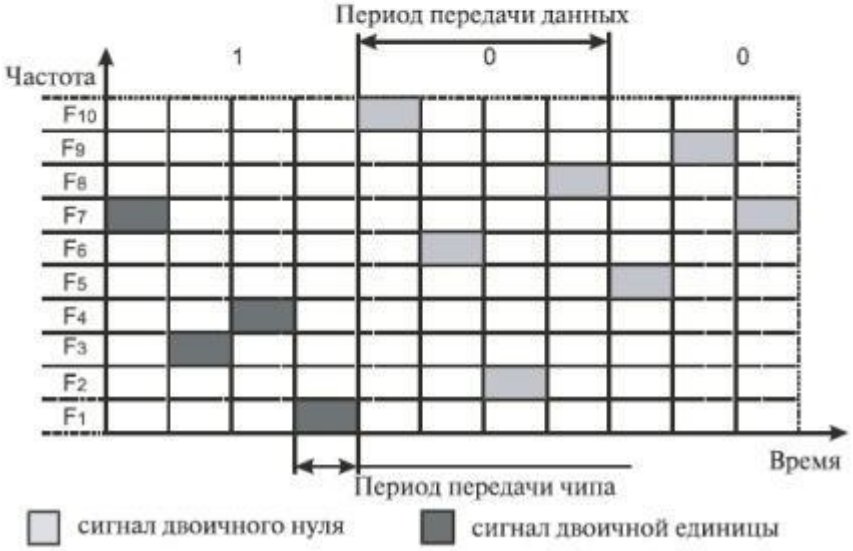
Расширение спектра скачкообразной перестройкой частоты

На каждой несущей частоте для передачи дискретной информации применяются стандартные методы модуляции, такие как FSK или PSK. Для того чтобы приемник синхронизировался с передатчиком, для обозначения начала каждого периода передачи в течение некоторого времени передаются синхробиты. Так что полезная скорость этого метода кодирования оказывается меньше из-за постоянных накладных расходов на синхронизацию.

Несущая частота меняется в соответствии с номерами частотных подканалов, вырабатываемых алгоритмом псевдослучайных чисел. Псевдослучайная последовательность зависит от некоторого параметра, который называют начальным числом. Если приемнику и передатчику известны алгоритм и значение начального числа, то они меняют частоты в одинаковой последовательности, называемой последовательностью псевдослучайной перестройки частоты. Если частота смены подканалов ниже, чем скорость передачи данных в канале, то такой режим называют: - медленным расширением спектра (рис.а); в противном случае мы имеем дело с - быстрым расширением спектра (рис.б).



а) Скорость передачи данных выше чиповой скорости



б) Скорость передачи данных ниже чиповой скорости

Метод быстрого расширения спектра более устойчив к помехам, поскольку узкополосная помеха, которая подавляет сигнал в определенном подканале, не приводит к потере бита, так как его значение повторяется несколько раз в различных частотных подканалах. В этом режиме не проявляется эффект межсимвольной интерференции, потому что ко времени прихода задержанного вдоль одного из путей сигнала система успевает перейти на другую частоту.

Метод медленного расширения спектра таким свойством не обладает, но зато он проще в реализации и сопряжен с меньшими накладными расходами.

В FHSS подход к использованию частотного диапазона не такой, как в других методах кодирования - вместо экономного расходования узкой полосы делается попытка занять весь доступный диапазон. На первый взгляд это кажется

не очень эффективным - ведь в каждый момент времени в диапазоне работает только один канал. Однако последнее утверждение не всегда справедливо - коды расширенного спектра можно использовать и для мультиплексирования нескольких каналов в широком диапазоне. В частности, методы FHSS позволяют организовать одновременную работу нескольких каналов путем выбора для каждого канала таких псевдослучайных последовательностей, чтобы в каждый момент времени каждый канал работал на своей частоте (конечно, это можно сделать, только если число каналов не превышает числа частотных подканалов).

Методы FHSS используются в беспроводных технологиях IEEE 802.11 и Bluetooth.

Прямое последовательное расширение спектра (Direct Sequence Spread Spectrum - DSSS)
(кодовое разделение)

В методе прямого последовательного расширения спектра также используется весь частотный диапазон, выделенный для одной беспроводной линии связи. В отличие от метода FHSS, весь частотный диапазон занимается не за счет постоянных переключений с частоты на частоту, а за счет того, что каждый бит информации заменяется N-битами, так что тактовая скорость передачи сигналов увеличивается в N раз. А это, в свою очередь, означает, что спектр сигнала также расширяется в N раз. Достаточно соответствующим образом выбрать скорость передачи данных и значение N, чтобы спектр сигнала заполнил весь диапазон.

В данной схеме все передатчики транслируют сигналы на одной и той же частоте **f**, в области **s** и во время **t**, но с разными кодами $\mathbf{C_i}$.

Цель кодирования методом DSSS та же, что и методом FHSS, - повышение устойчивости к помехам. Узкополосная помеха будет искажать только определенные частоты спектра сигнала, так что приемник с большой степенью вероятности сможет правильно распознать передаваемую информацию.

Код, которым заменяется двоичная единица исходной информации, называется расширяющей последовательностью или CDM-символом **(Code Division Multiplexing - CDM)** - кодовая последовательность длиной в 11, 16, 32, 64 и т. п. бит. Расширяющая последовательность уникальна для каждого передатчика. Как правило, если для замены "1" в исходном потоке данных

используют некий CDM-код, то для замены "0" применяют тот же код, но инвертированный.

Каждый бит такой расширяющей последовательности называется **чипом**.

Соответственно, скорость передачи результирующего кода называют **чиповой скоростью**.

Двоичный нуль кодируется инверсным значением расширяющей последовательности.

Приемник знает CDM-код передатчика, сигналы которого должен воспринимать. Он постоянно принимает все сигналы и оцифровывает их. Затем в специальном устройстве (корреляторе) производится операция свертки (умножения с накоплением) входного оцифрованного сигнала с известным ему CDM-кодом и его инверсией. В несколько упрощенном виде это выглядит как операция скалярного произведения вектора входного сигнала и вектора с CDM-кодом. Если сигнал на выходе коррелятора превышает некий установленный пороговый уровень, приемник считает, что принял 1 или 0.

Для увеличения вероятности приема передатчик может повторять посылку каждого бита несколько раз.

При этом сигналы других передатчиков с другими CDM-кодами приемник воспринимает как аддитивный шум.

Более того, благодаря большой избыточности (каждый бит заменяется десятками чипов), мощность принимаемого сигнала может быть сопоставима с интегральной мощностью шума. Сходства CDM-сигналов со случайным (гауссовым) шумом добиваются, используя CDM-коды, порожденные генератором псевдослучайных последовательностей.

Количество битов в расширяющей последовательности определяет коэффициент расширения исходного кода. Как и в случае FHSS, для кодирования битов результирующего кода может использоваться любой вид модуляции, например BPSK (*binary phase-shift keying).*

Чем больше коэффициент расширения, тем шире спектр результирующего сигнала и выше степень подавления помех. Но при этом растет занимаемый каналом диапазон спектра. Обычно коэффициент расширения имеет значение от 10 до 100.

Наиболее сильная сторона данного уплотнения заключается в повышенной защищенности и скрытности передачи данных: не зная кода, невозможно получить сигнал, а в ряде случаев - и обнаружить его присутствие. Кроме того, кодовое пространство несравненно более значительно по сравнению с частотной схемой уплотнения, что позволяет без особых проблем присваивать каждому передатчику свой индивидуальный код. Основной же проблемой кодового уплотнения до недавнего времени являлась сложность технической реализации приемников и необходимость обеспечения точной синхронизации передатчика и приемника для гарантированного получения пакета.

Очень часто в качестве значения расширяющей последовательности берут последовательность Баркера (Barker), которая состоит из 11 бит: 10110111000 (5B8)h. Если передатчик использует эту последовательность, то передача трех битов 110 ведет к передаче следующих битов:

10110111000 10110111000 01001000111.

Последовательность Баркера позволяет приемнику быстро синхронизироваться с передатчиком, то есть надежно выявлять начало последовательности. Приемник определяет такое событие, поочередно сравнивая получаемые биты с образцом последовательности. Действительно, если сравнить последовательность Баркера с такой же последовательностью, но сдвинутой на один бит влево или вправо, мы получим меньше половины совпадений значений битов.

	1	0	1	1	0	1	1	1	0	0	0	
1	0	1	1	0	1	1	1	0	0	0		
			X			X	X		X	X		
	1	0	1	1	0	1	1	1	0	0	0	
		1	0	1	1	0	1	1	1	0	0	0
				X			X	X		X	X	

Значит, даже при искажении нескольких битов с большой долей вероятности приемник правильно определит начало последовательности, а значит, сможет правильно интерпретировать получаемую информацию.

Метод DSSS в меньшей степени защищен от помех, чем метод быстрого расширения спектра, так как мощная узкополосная помеха влияет на часть спектра, а значит, и на результат распознавания единиц или нулей.

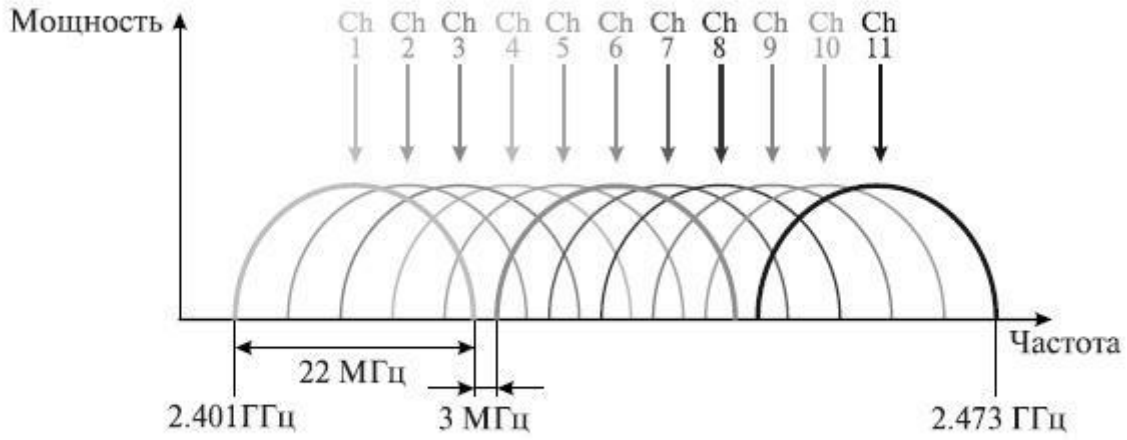


Рис. 1.12. Каналы, используемые в технологии DSSS

Беспроводные локальные сети DSSS используют каналы шириной 22 МГц, благодаря чему многие WLAN могут работать в одной и той же зоне покрытия. В Северной Америке и большей части Европы, в том числе и в России, каналы шириной 22 МГц позволяют создать в диапазоне 2,4- 2,473 ГГц три неперекрывающихся канала передачи.

Метод мультиплексирования посредством ортогональных несущих частот (Orthogonal Frequency Division Multiplexing - OFDM)

Суть этого механизма: весь доступный частотный диапазон разбивается на достаточно много поднесущих (от нескольких сот до тысяч). Одному каналу связи (приемнику и передатчику) назначают для передачи несколько таких несущих, выбранных из множества по определенному закону. Передача ведется одновременно по всем поднесущим, т. е. в каждом передатчике исходящий поток данных разбивается на N субпотоков, где N - число поднесущих, назначенных данному передатчику.

Распределение поднесущих в ходе работы может динамически изменяться, что делает данный механизм не менее гибким, чем метод временного уплотнения.

Схема OFDM имеет несколько преимуществ. Во-первых, селективному замиранию будут подвержены только некоторые подканалы, а не весь сигнал.

Если поток данных защищен кодом прямого исправления ошибок, то с этим замиранием легко бороться. Во-вторых, что более важно, OFDM позволяет подавить межсимвольную интерференцию. Межсимвольная интерференция оказывает значительное влияние при высоких скоростях передачи данных, так как расстояние между битами (или символами) мало. В схеме OFDM скорость передачи данных уменьшается в N раз, что позволяет увеличить время передачи символа в N раз. Таким образом, если время передачи символа для исходного потока составляет T_s, то период сигнала OFDM будет равен NT_s. Это позволяет существенно снизить влияние межсимвольных помех. При проектировании системы N выбирается таким образом, чтобы величина NT_s значительно превышала среднеквадратичный разброс задержек канала.

Лекция 3. Цифровая манипуляция

Манипуляция (цифровая модуляция) — в теории передачи дискретных сообщений процесс преобразования последовательности кодовых символов в последовательность элементов сигнала (частный случай модуляции — при дискретных уровнях модулирующего сигнала).

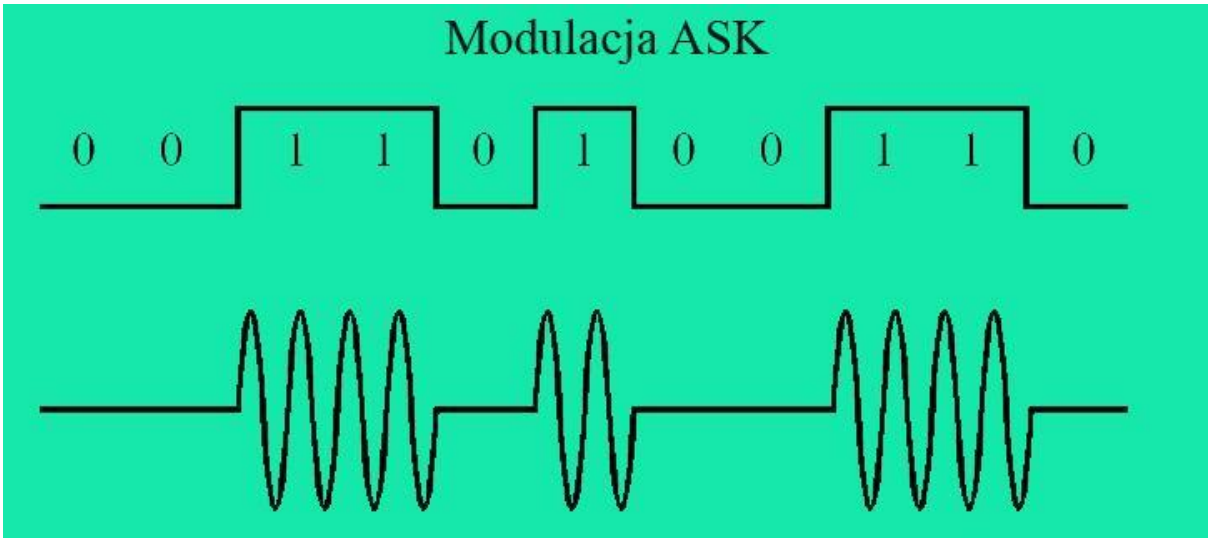
Виды манипуляций

Существуют следующие типы манипуляций:

- Частотная манипуляция
- Фазовая манипуляция
- Амплитудная манипуляция
- Квадратурная амплитудная манипуляция

Амплитудная манипуляция

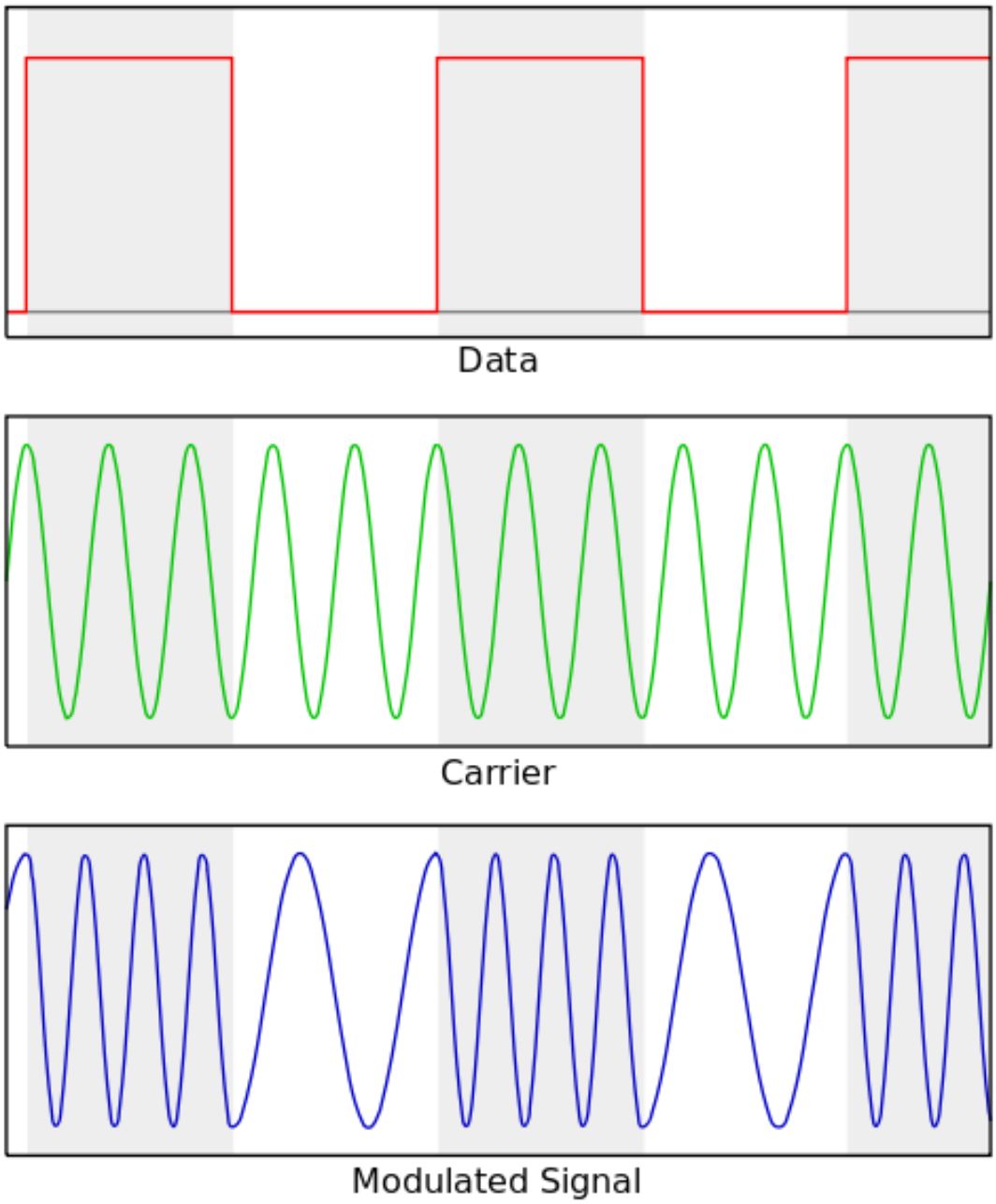
Амплитудная манипуляция (АМн; англ. amplitude shift keying (ASK) — изменение сигнала, при котором скачкообразно меняется амплитуда несущего колебания.



Частотная манипуляция

При **частотной манипуляции** (ЧМн, англ. *Frequency Shift Keying (FSK)*) значениям «0» и «1» информационной последовательности соответствуют определённые частоты синусоидального сигнала при неизменной амплитуде. Частотная манипуляция весьма помехоустойчива, поскольку помехи телефонного канала искажают в основном амплитуду, а не частоту сигнала. Однако при частотной манипуляции неэкономно расходуется ресурс полосы частот телефонного канала. Поэтому этот вид модуляции применяется в низкоскоростных протоколах, позволяющих осуществлять связь по каналам с низким отношением сигнал/шум.

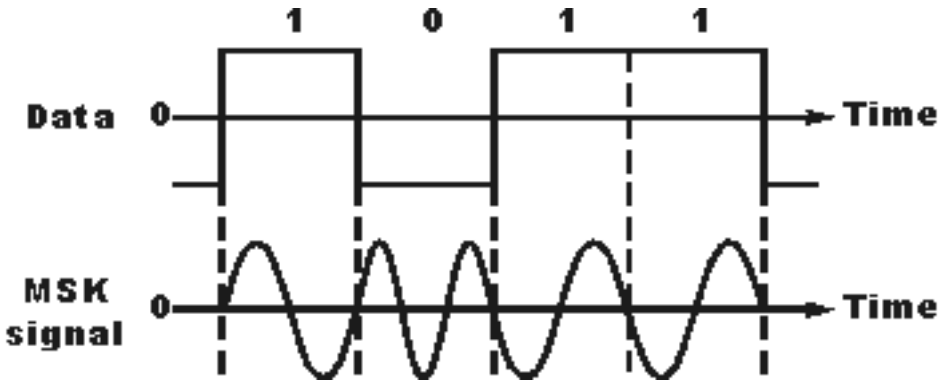
Частотная манипуляция с минимальным сдвигом (англ. *Minimal Shift Keying (MSK)*) представляет собой способ модуляции, при котором не происходит скачков фазы и изменение частоты происходит в моменты пересечения несущей нулевого уровня. MSK уникальна потому, что значение частот соответствующих логическим «0» и «1» отличаются на величину равную половине скорости передачи данных. Другими словами, индекс модуляции равен 0,5:



Например, при скорости передачи 1200 бит/с MSK-сигнал будет сформирован из колебаний с частотами 1200 Гц и 1800 Гц соответствующих логическим «0» и «1».

В телеграфировании: **Частотная манипуляция** процесс изменения частоты генератора в соответствии с передающими посылками

Гауссовская частотная модуляция с минимальным сдвигом (англ. *Gaussian Minimum Shift Keying (GMSK)*)



Перед модуляцией последовательность из прямоугольных импульсов данных проходит через Гауссовский фильтр.

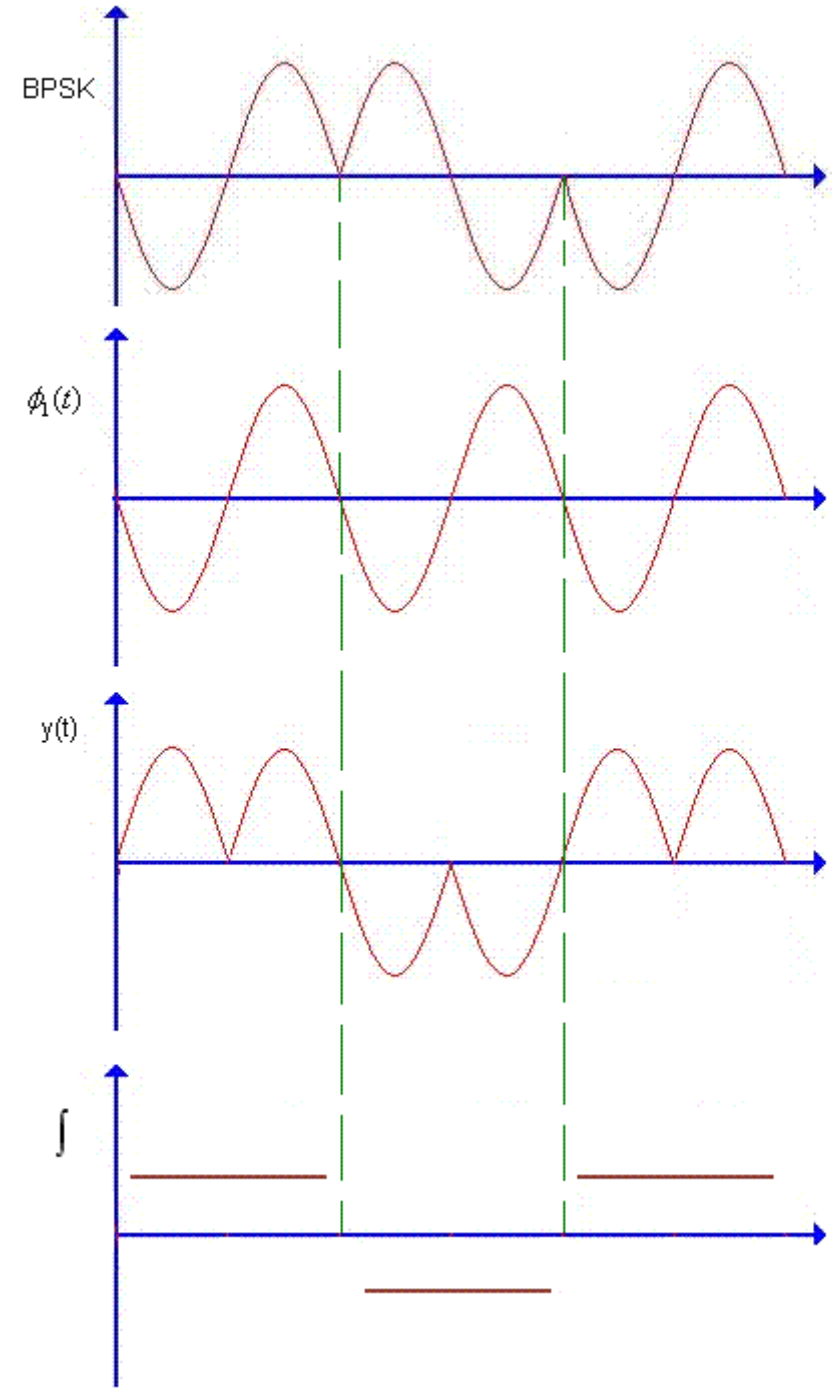
Преимущество данного вида модуляции в том, что он имеет минимальный уровень излучения на боковых и зеркальных частотах, то есть не мешает другим пользователям эфира. Плотность информации — 1 бит на символ или на герц. Данный вид модуляции, как и MSK, относится к частотным видам модуляции с непрерывной фазой (англ. *continuous phase frequency-shift keying, CPFSK*).

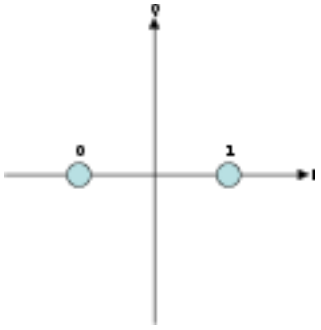
Модулирующий сигнал получается путём преобразования информационного потока из вида 0/1 в вид −1/+1. Затем −1/+1 сигнал фильтруется таким образом, что сформированный +1/-1 прямоугольный сигнал преобразуется в сигналы имеющие форму гауссовского импульса. Далее полученный сигнал подается на ЧМ модулятор с индексом модуляции равным 0,5, и таким образом образуется полный сигнал GMSK. Это очень простой метод, но выполнить требование точности индекса модуляции на практике сложно. Обычно используют квадратурный модулятор, в котором «тяжесть» переносится на фазовращатель для фильтрованного сигнала, что для цифровых схем сложности не представляет. Если гауссовские импульсы не накладываются, то вид модуляции называют 1-GMSK. Если — накладываются на 50 % (½), то модуляцию называют 2-GMSK, и так далее. Чем больше наложение битов, тем более существенны межсимвольные искажения между соседними битами.

Используется для передачи данных в стандартах GSM, DECT, CDPD и Mobitex.

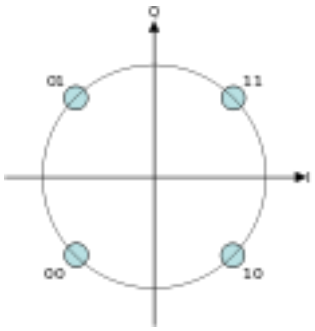
Фазовая манипуляция

Фазовая манипуляция (ФМн, англ. phase-shift keying (PSK)) — один из видов фазовой модуляции, при которой фаза несущего колебания меняется скачкообразно в зависимости от информационного сообщения.





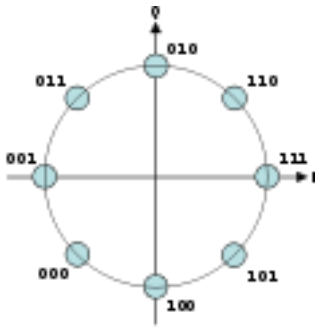
Двоичная фазовая манипуляция (BPSK)



Квадратурная фазовая манипуляция (QPSK)

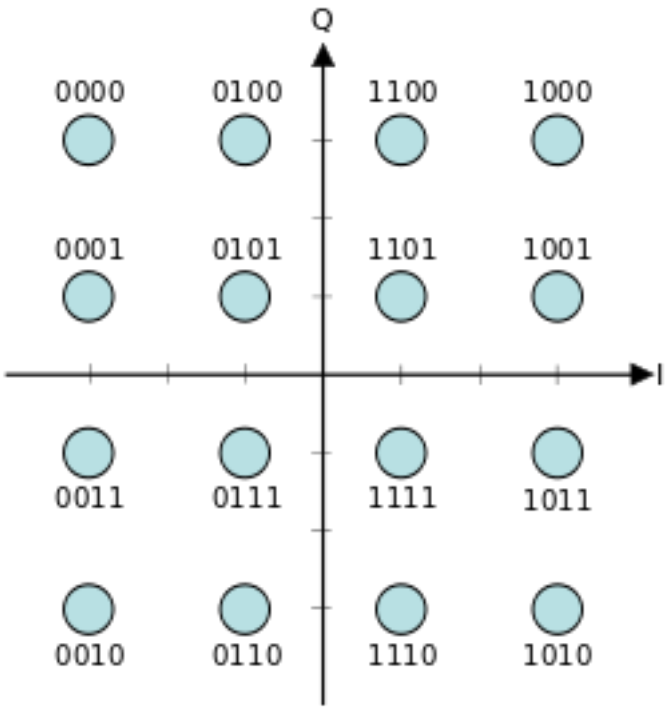
При **квадратурной фазовой манипуляции** (англ. *QPSK — Quadrature Phase Shift Keying* или 4-PSK) используется созвездие из четырёх точек, размещённых на равных расстояниях на окружности. Используя 4 фазы, в QPSK на символ приходится два бита, как показано на рисунке. Анализ показывает, что скорость может быть увеличена в два раза относительно BPSK при той же полосе сигнала, либо оставить скорость прежней, но уменьшить полосу вдвое.

Хотя QPSK можно считать квадратурной манипуляцией (QAM-4), иногда её проще рассматривать в виде двух независимых модулированных несущих, сдвинутых на 90°. При таком подходе чётные (нечётные) биты используются для модуляции синфазной составляющей I {\displaystyle I}, а нечётные (чётные) — квадратурной составляющей несущей Q {\displaystyle Q} . Так как BPSK используется для обеих составляющих несущей, то они могут быть демодулированы независимо.



Восьмеричная фазовая манипуляция (8-PSK)

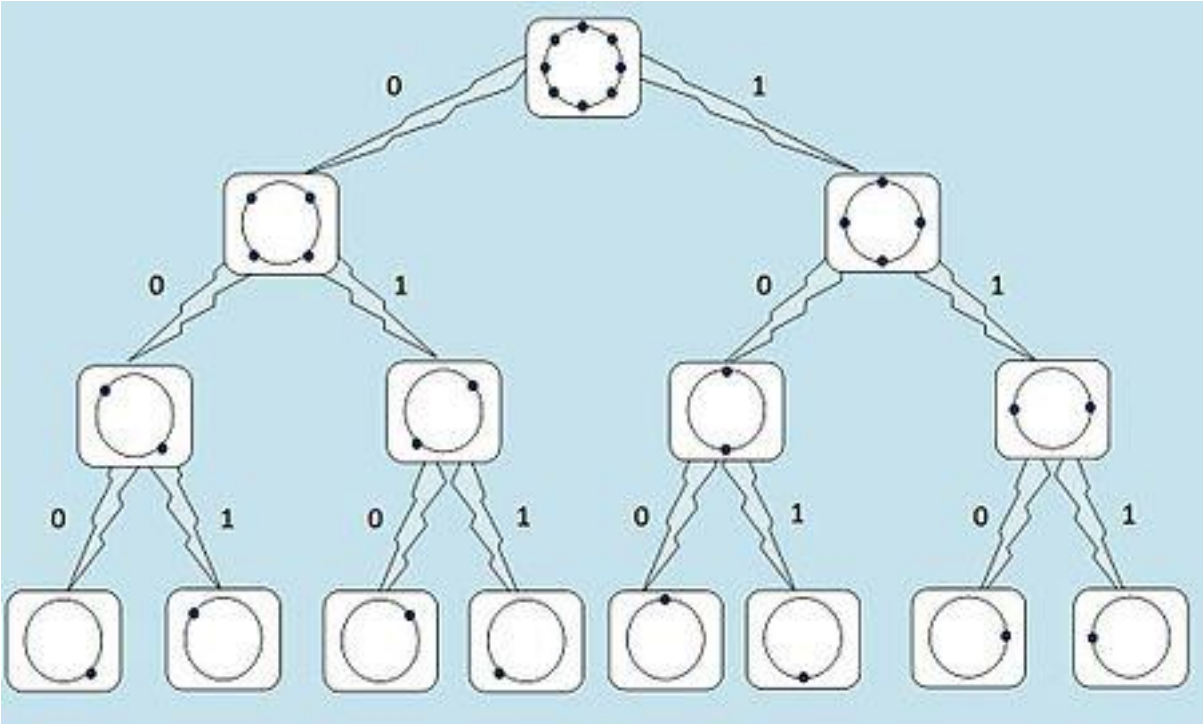
Квадратурная амплитудная манипуляция



Сигнальное созвездие 16-ти позиционного КАМн сигнала (16-QAM с применением кодов Грея)

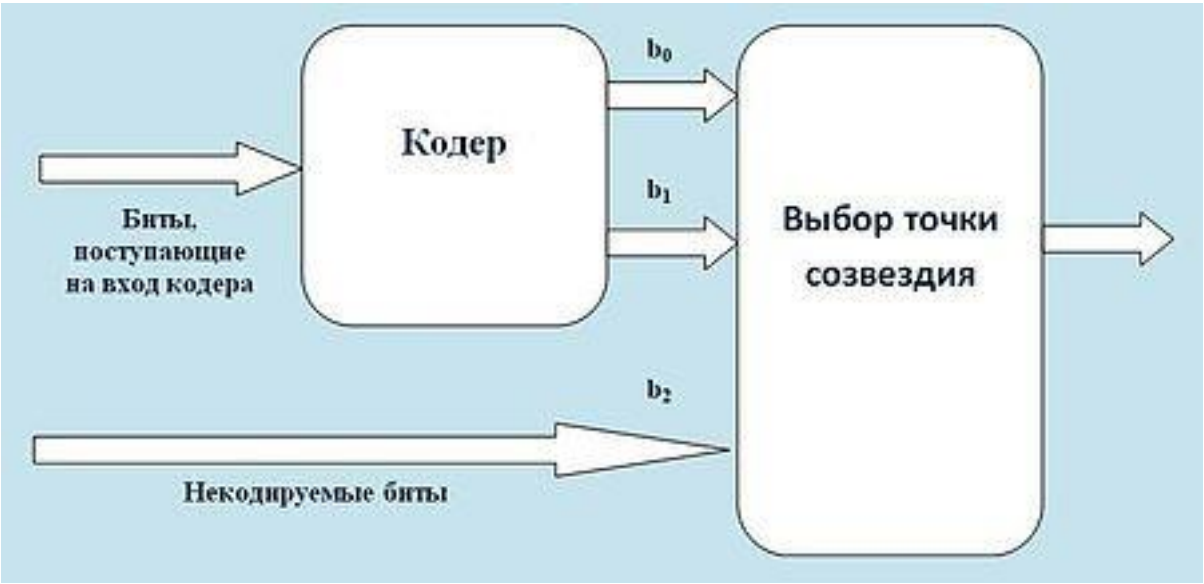
Квадратурная амплитудная манипуляция (КАМ, англ. Quadrature amplitude modulation (QAM)) — манипуляция, при которой изменяется как фаза, так и амплитуда сигнала, что позволяет увеличить количество информации, передаваемой одним состоянием (отсчётом) сигнала. В англоязычной литературе такой тип манипуляции часто называют QAM, обозначение QASK применяется редко.

Решётчатая кодированная модуляция



Разделение 8-фазового созвездия для решётчатой кодированной модуляции

При использовании блочного или свёрточного кодирования помехоустойчивость радиосвязи повышается за счёт расширения полосы частоты и усложнения радиоаппаратуры без повышения отношения сигнал/шум (ОСШ). Для сохранения помехоустойчивости при том же значении ОСШ можно уменьшить используемую полосу частот и упростить радиоаппаратуру с помощью применения решётчатой кодированной модуляции (ТСМ), которая впервые была разработана в 1982 году Унгербоком. В основе ТСМ лежит совместный процесс кодирования и манипуляции.



Лекция 4. Стандарт 802.11 (WiFi). Уровень доступа к среде

Стек протоколов IEEE 802.11.

Естественно, стек протоколов стандарта IEEE 802.11 соответствует общей структуре стандартов комитета 802, то есть 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, то есть физическим уровнем и уровнем MAC, а уровень LLC выполняет свои стандартные общие для всех технологий LAN функции (рис. 2.1).

На физическом уровне существует несколько вариантов спецификаций, которые отличаются используемым частотным диапазоном, методом кодирования и как следствие - скоростью передачи данных. Все варианты физического уровня работают с одним и тем же алгоритмом уровня MAC, но некоторые временные параметры уровня MAC зависят от используемого физического уровня.

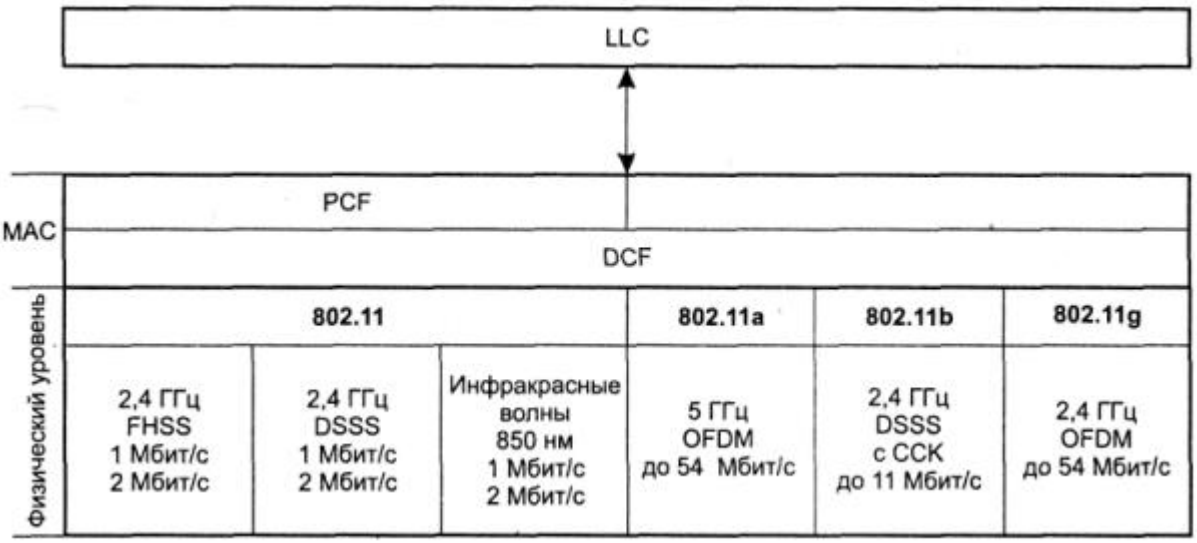


Рис. 2.1. Стек протоколов IEEE 802.11

Уровень доступа к среде стандарта 802.11

В сетях 802.11 уровень MAC обеспечивает два режима доступа к разделяемой среде

(рис. 2.1):

- распределенный режим DCF (Distributed Coordination Function);
- централизованный режим PCF (Point Coordination Function).

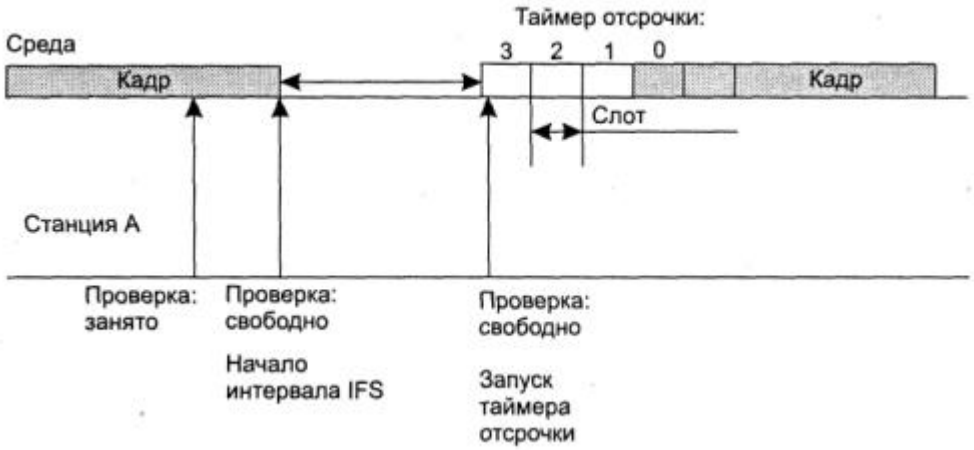
1) Распределенный режим доступа DCF

Рассмотрим сначала, как обеспечивается доступ в распределенном режиме DCF. В этом режиме реализуется метод множественного доступа с контролем несущей и предотвращением коллизий (Carrier Sense Multiple Access with Collision Avoidance - CSMA/CA). Вместо неэффективного в беспроводных сетях прямого распознавания коллизий по методу CSMA/CD здесь используется их косвенное выявление. Для этого каждый переданный кадр должен подтверждаться кадром положительной квитанции, посылаемым станцией назначения. Если же по истечении оговоренного тайм-аута квитанция не поступает, станция-отправитель считает, что произошла коллизия.

Режим доступа DCF требует синхронизации станций. В спецификации 802.11 эта проблема решается достаточно элегантно - временные интервалы начинают отсчитываться от момента окончания передачи очередного кадра (рис. 2.2). Это не требует передачи каких-либо специальных синхронизирующих сигналов и не ограничивает размер пакета размером слота, так как слоты принимаются во внимание только при принятии решения о начале передачи кадра.

Станция, которая хочет передать кадр, обязана предварительно прослушать среду. Стандарт IEEE 802.11 предусматривает два механизма контроля активности в канале (обнаружения несущей): физический и виртуальный. Первый механизм реализован на физическом уровне и сводится к определению уровня сигнала в антенне и сравнению его с пороговой величиной. Виртуальный механизм обнаружения несущей основан на том, что в передаваемых кадрах данных, а также в управляющих кадрах ACK и RTS/CTS содержится информация о времени, необходимом для передачи пакета (или группы пакетов) и получения подтверждения. Все устройства сети получают информацию о текущей передаче и могут определить, сколько времени канал будет занят, т.е. устройство при установлении связи сообщает всем, на какое время оно резервирует канал. Как

только станция фиксирует окончание передачи кадра, она обязана отсчитать интервал времени, равный межкадровому интервалу (IFS). Если после истечения IFS среда все еще свободна, начинается отсчет слотов фиксированной длительности. Кадр можно передавать только в начале какого-либо из слотов при условии, что среда свободна. Станция выбирает для передачи слот на основании усеченного экспоненциального двоичного алгоритма отсрочки, аналогичного используемому в методе CSMA/CD. Номер слота выбирается как случайное целое число, равномерно распределенное в интервале [0, CW], где "CW" означает "Contention Window" (конкурентное окно).



Рассмотрим этот довольно непростой метод доступа на примере рисунка 2.2. Пусть станция А выбрала для передачи на основании усеченного экспоненциального двоичного алгоритма отсрочки слот 3. При этом она присваивает таймеру отсрочки (назначение которого будет ясно из дальнейшего описания) значение 3 и начинает проверять состояние среды в начале каждого слота. Если среда свободна, то из значения таймера отсрочки вычитается 1, и если результат равен нулю, начинается передача кадра.

Таким образом, обеспечивается условие незанятости всех слотов, включая выбранный. Это условие является необходимым для начала передачи.

Если же в начале какого-нибудь слота среда оказывается занятой, то вычитания единицы не происходит, и таймер "замораживается". В этом случае станция начинает новый цикл доступа к среде, изменяя только алгоритм выбора слота для передачи. Как и в предыдущем цикле, станция следит за средой и при ее

освобождении делает паузу в течение межкадрового интервала. Если среда осталась свободной, то станция использует значение "замороженного" таймера в качестве номера слота и выполняет описанную выше процедуру проверки свободных слотов с вычитанием единиц, начиная с замороженного значения таймера отсрочки.

Размер слота зависит от способа кодирования сигнала; так, для метода FHSS размер слота равен 28 мкс, а для метода DSSS - 1 мкс. Размер слота выбирается таким образом, чтобы он превосходил время распространения сигнала между любыми двумя станциями сети плюс время, затрачиваемое станцией на распознавание занятости среды. Если такое условие соблюдается, то каждая станция сети сумеет правильно распознать начало передачи кадра при прослушивании слотов, предшествующих выбранному ею для передачи слоту. Это, в свою очередь, означает следующее.

Коллизия может иметь место только в том случае, когда несколько станций выбирают один и тот же слот для передачи.

В этом случае кадры искажаются, и квитанции от станций назначения не приходят. Не получив в течение определенного времени квитанцию, отправители фиксируют факт коллизии и пытаются передать свои кадры снова. При каждой повторной неудачной попытке передачи кадра интервал [0, CW], из которого выбирается номер слота, удваивается. Если, например, начальный размер окна выбран равным 8 (то есть CW = 7), то после первой коллизии размер окна должен быть равен 16 (CW = 15), после второй последовательной коллизии - 32 и т. д. Начальное значение CW, в соответствии со стандартом 802.11, должно выбираться в зависимости от типа физического уровня, используемого в беспроводной локальной сети.

Как и в методе CSMA/CD, в данном методе количество неудачных попыток передачи одного кадра ограничено, но стандарт 802.11 не дает точного значения этого верхнего предела. Когда верхний предел в N попыток достигнут, кадр отбрасывается, а счетчик последовательных коллизий устанавливается в нуль. Этот счетчик также устанавливается в нуль, если кадр после некоторого количества неудачных попыток все же передается успешно.

В беспроводных сетях возможна ситуация, когда два устройства (A и B) удалены и не слышат друг друга, однако оба попадают в зону охвата третьего устройства C (рис. 2.3) - так называемая проблема скрытого терминала. Если оба устройства A и B начнут передачу, то они принципиально не смогут обнаружить конфликтную ситуацию и определить, почему пакеты не проходят.

Рис. 2.3. Проблема скрытого терминала

В режиме доступа DCF применяются меры для устранения эффекта скрытого терминала. Для этого станция, которая хочет захватить среду и в соответствии с описанным алгоритмом начинает передачу кадра в определенном слоте, вместо кадра данных сначала посылает станции назначения короткий служебный кадр RTS (Request To Send - запрос на передачу). На этот запрос станция назначения должна ответить служебным кадром CTS (Clear To Send - свободна для передачи), после чего станция-отправитель посылает кадр данных. Кадр CTS должен оповестить о захвате среды те станции, которые находятся вне зоны сигнала станции-отправителя, но в зоне досягаемости станции-получателя, то есть являются скрытыми терминалами для станции-отправителя.

Максимальная длина кадра данных 802.11 равна 2346 байт, длина RTS-кадра - 20 байт, CTS-кадра - 14 байт. Так как RTS- и CTS-кадры гораздо короче, чем кадр данных, потери данных в результате коллизии RTS- или CTS-кадров гораздо меньше, чем при коллизии кадров данных. Процедура обмена RTS- и CTS-кадрами не обязательна. От нее можно отказаться при небольшой нагрузке сети, поскольку в такой ситуации коллизии случаются редко, а значит, не стоит тратить дополнительное время на выполнение процедуры обмена RTS- и CTS-кадрами.

При помехах иногда случается, что теряются большие фреймы данных, поэтому можно уменьшить длину этих фреймов путем фрагментации. Фрагментация фрейма - это выполняемая на уровне MAC функция, назначение которой - повысить надежность передачи фреймов через беспроводную среду. Под фрагментацией понимается дробление фрейма на меньшие фрагменты и передача каждого из них отдельно (рис. 2.4).

Предполагается, что вероятность успешной передачи меньшего фрагмента через зашумленную беспроводную среду выше. Получение каждого фрагмента фрейма подтверждается отдельно; следовательно, если какой-нибудь фрагмент фрейма будет передан с ошибкой или вступит в коллизию, передавать повторно придется только его, а не весь фрейм. Это увеличивает пропускную способность среды.

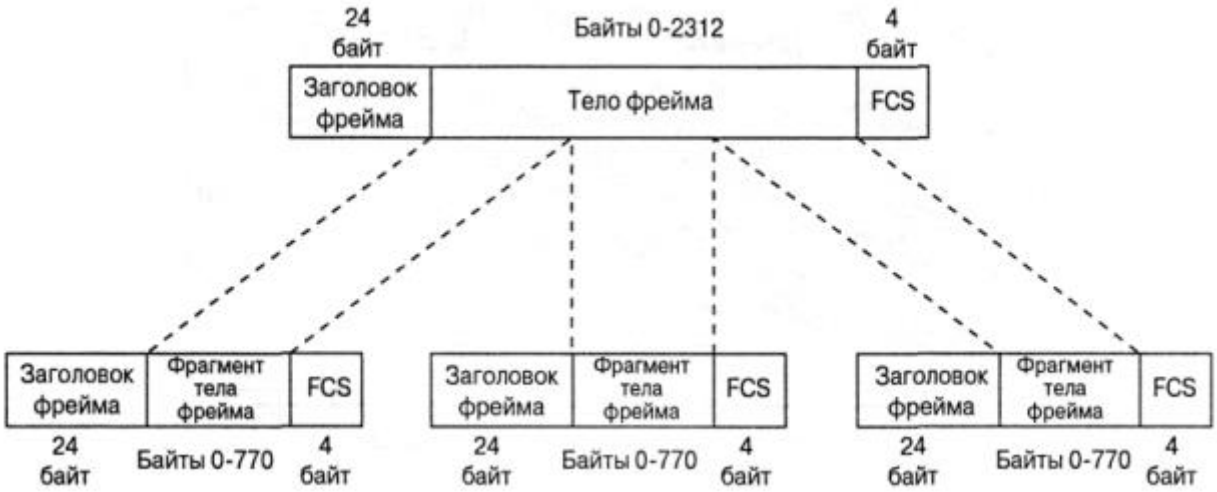


Рис. 2.4. Фрагментация фрейма

Размер фрагмента может задавать администратор сети. Фрагментации подвергаются только одноадресные фреймы. Широковещательные, или многоадресные, фреймы передаются целиком. Кроме того, фрагменты фрейма передаются пакетом, с использованием только одной итерации механизма доступа к среде DCF.

Хотя за счет фрагментации можно повысить надежность передачи фреймов в беспроводных локальных сетях, она приводит к увеличению "накладных расходов" MAC-протокола стандарта 802.11. Каждый фрагмент фрейма включает информацию, содержащуюся в заголовке 802.11 MAC, а также требует передачи

соответствующего фрейма подтверждения. Это увеличивает число служебных сигналов MAC-протокола и снижает реальную производительность беспроводной станции. Фрагментация - это баланс между надежностью и непроизводительной загрузкой среды.

Централизованный режим доступа PCF

В том случае, когда в сети имеется станция, выполняющая функции точки доступа, может также применяться централизованный режим доступа PCF, обеспечивающий приоритетное обслуживание трафика. В этом случае говорят, что точка доступа играет роль арбитра среды.

Режим доступа PCF в сетях 802.11 сосуществует с режимом DCF. Оба режима координируются с помощью трех типов межкадровых интервалов (рис. 2.5).

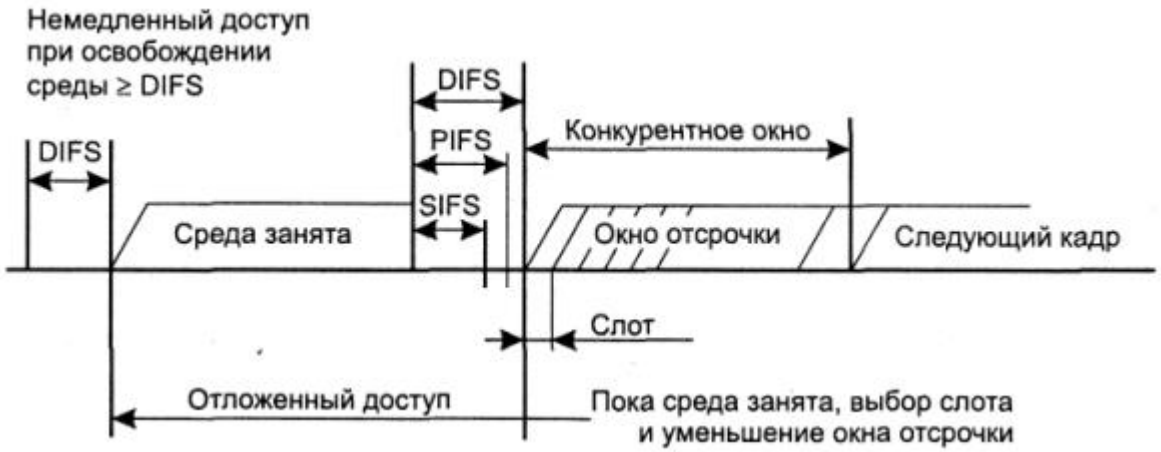


Рис. 2.5. Сосуществование режимов PCF и DCF

После освобождения среды каждая станция отсчитывает время простоя среды, сравнивая его с тремя значениями:

- короткий межкадровый интервал (Short IFS - SIFS);
- межкадровый интервал режима PCF (PIFS);
- межкадровый интервал режима DCF (DIFS).

Захват среды с помощью распределенной процедуры DCF возможен только в том случае, когда среда свободна в течение времени, равного или большего, чем DIFS. То есть в качестве IFS в режиме DCF нужно использовать интервал DIFS - самый

длительный период из трех возможных, что дает этому режиму самый низкий приоритет.

Межкадровый интервал SIFS имеет наименьшее значение, он служит для первоочередного захвата среды ответными CTS-кадрами или квитанциями, которые продолжают или завершают уже начавшуюся передачу кадра.

Значение межкадрового интервала PIFS больше, чем SIFS, но меньше, чем DIFS. Промежутком времени между завершением PIFS и DIFS пользуется арбитр среды. В этом промежутке он может передать специальный кадр, который говорит всем станциям, что начинается контролируемый период. Получив этот кадр, станции, которые хотели бы воспользоваться алгоритмом DCF для захвата среды, уже не могут этого сделать, они должны дожидаться окончания контролируемого периода. Его длительность объявляется в специальном кадре, но этот период может закончиться и раньше, если у станций нет чувствительного к задержкам трафика. В этом случае арбитр передает служебный кадр, после которого по истечении интервала DIFS начинает работать режим DCF.

На управляемом интервале реализуется централизованный метод доступа PCF. Арбитр выполняет процедуру опроса, чтобы по очереди предоставить каждой такой станции право на использование среды, направляя ей специальный кадр. Станция, получив такой кадр, может ответить другим кадром, который подтверждает прием специального кадра и одновременно передает данные (либо по адресу арбитра для транзитной передачи, либо непосредственно станции).

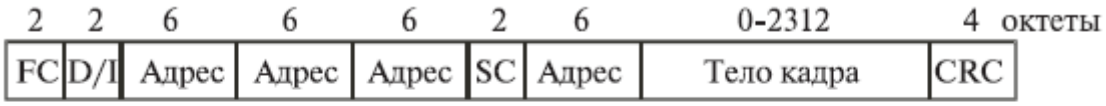
Для того чтобы какая-то доля среды всегда доставалась асинхронному трафику, длительность контролируемого периода ограничена. После его окончания арбитр передает соответствующий кадр и начинается неконтролируемый период.

Каждая станция может работать в режиме PCF, для этого она должна подписаться на данную услугу при присоединении к сети.

Кадр MAC-подуровня

На рис. 2.6 изображен формат кадра 802.11. Приведенная общая структура применяется для всех информационных и управляющих кадров, хотя не все поля

используются во всех случаях.



FC — управление кадром
D/I — идентификатор длительности/соединения
SC — управление очередностью

Рис. 2.6. Формат кадра MAC IEEE 802.11

Перечислим поля общего кадра:

- Управление кадром. Указывается тип кадра и предоставляется управляющая информация (объясняется ниже).
- Идентификатор длительности/соединения. Если используется поле длительности, указывается время (в микросекундах), на которое требуется выделить канал для успешной передачи кадра MAC. В некоторых кадрах управления в этом поле указывается идентификатор ассоциации или соединения.
- Адреса. Число и значение полей адреса зависит от контекста. Возможны следующие типы адреса: источника, назначения, передающей станции, принимающей станции.
- Управление очередностью. Содержит 4-битовое подполе номера фрагмента, используемое для фрагментации и повторной сборки, и 12-битовый порядковый номер, используемый для нумерации кадров, передаваемых между приемником и передатчиком.
- Тело кадра. Содержит модуль данных протокола LLC или управляющую информацию MAC.
- Контрольная последовательность кадра. 32-битовая проверка четности с избыточностью.

Поле управления кадром, показанное на рис. 2.7, состоит из следующих полей:

- Версия протокола. Версия 802.11, текущая версия - 0.
- Тип. Определим тип кадра: контроль, управление или данные.

- Подтип. Дальнейшая идентификация функций кадра. Разрешенные сочетания типов и подтипов перечислены в таблице 2.1.

Таблица 2.1. Разрешенные комбинации типа и подтипа

Значение типа	Описание типа	Значение подтипа	Описание подтипа
00	Управление	0000	Запрос ассоциации
00	Управление	0001	Ответ на запрос ассоциации
00	Управление	0010	Запрос повторной ассоциации
00	Управление	0011	Ответ на запрос повторной ассоциации
00	Управление	0100	Пробный запрос
00	Управление	0101	Ответ на пробный запрос
00	Управление	1000	Сигнальный кадр
00	Управление	1001	Объявление наличия трафика
00	Управление	1010	Разрыв ассоциации
00	Управление	1011	Аутентификация
00	Управление	1100	Отмена аутентификации
01	Контроль	1010	PS-опрос
01	Контроль	1011	Запрос передачи
01	Контроль	1100	"Готов к передаче"
01	Контроль	1101	Подтверждение
01	Контроль	1110	Без состязания (CF)-конец
01	Контроль	1111	CF-конец + CF-подтверждение
10	Данные	0000	Данные
10	Данные	0001	Данные + CF-подтверждение
10	Данные	0010	Данные + CF-опрос
10	Данные	0011	Данные + CF-подтверждение + CF-опрос
10	Данные	0100	Нулевая функция (без данных)
10	Данные	0101	Данные + CF-подтверждение
10	Данные	0110	Данные + CF-опрос
10	Данные	0111	Данные + CF-подтверждение +

- К DS. Координационная функция MAC присваивает этому биту значение 1, если кадр предназначен распределительной системе.
- От DS. Координационная функция MAC присваивает этому биту значение 0, если кадр исходит от распределительной системы.
- Больше фрагментов. 1, если за данным фрагментом следует еще несколько.
- Повтор. 1, если данный кадр является повторной передачей предыдущего.
- Управление мощностью. 1, если передающая станция находится в режиме ожидания.
- Больше данных. Указывает, что станция передала не все данные. Каждый блок данных может передаваться как один кадр или как группа фрагментов в нескольких кадрах.
- WEP. 1, если реализован алгоритм конфиденциальности проводного эквивалента (Wired Equivalent Privacy - WEP). Протокол WEP используется для обмена ключами шифрования при безопасном обмене данными.
- Порядок. 1, если используется услуга строгого упорядочения, указывающая адресату, что кадры должны обрабатываться строго по порядку.

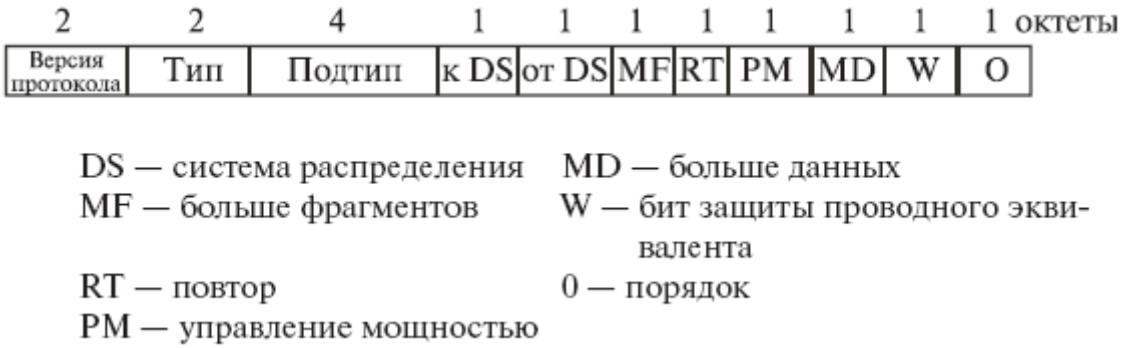


Рис. 2.7. Поле управления кадром

Рассмотрим теперь различные типы кадров MAC.

Контрольные кадры

Контрольные кадры способствуют надежной доставке информационных кадров. Существует шесть подтипов контрольных кадров:

- Опрос после выхода из экономичного режима (PS-опрос). Данный кадр

передается любой станцией станции, включающей точку доступа. В кадре запрашивается передача кадра, прибывшего, когда станция находилась в режиме энергосбережения, и в данный момент размещенного в буфере точки доступа.

- Запрос передачи (RTS). Данный кадр является первым из четверки, используемой для обеспечения надежной передачи данных. Станция, пославшая это сообщение, предупреждает адресата и остальные станции, способные принять данное сообщение, о своей попытке передать адресату информационный кадр.
- "Готов к передаче" (CTS). Второй кадр четырехкадровой схемы. Передается станцией-адресатом станции-источнику и предоставляет право отправки информационного кадра.
- Подтверждение (ACK). Подтверждение успешного приема предыдущих данных, кадра управления или кадра "PS-опрос".
- Без состязания (CF-конец). Объявляет конец периода без состязания; часть стратегии использования распределенного режима доступа.
- CF-конец + CF-подтверждение. Подтверждает кадр "CF-конец". Данный кадр завершает период без состязания и освобождает станции от ограничений, связанных с этим периодом.

Информационные кадры

Существует восемь подтипов информационных кадров, собранных в две группы. Первые четыре подтипа определяют кадры, переносящие данные высших уровней от исходной станции к станции-адресату. Перечислим эти кадры:

- Данные. Просто информационный кадр. Может использоваться как в период состязания, так и в период без состязания.
- Данные + CF-подтверждение. Может передаваться только в период без состязания. Помимо данных, в этом кадре имеется подтверждение полученной ранее информации.
- Данные + CF-опрос. Используется точечным координатором для доставки данных к мобильной станции и для запроса у мобильной станции информационного кадра, который находится в ее буфере.
- Данные + CF-подтверждение + CF-опрос. Объединяет в одном кадре функции

двух описанных выше кадров.

Остальные четыре подтипа информационных кадров фактически не переносят данные пользователя. Информационный кадр "нулевая функция" не переносит ни данных, ни запросов, ни подтверждений. Он используется только для передачи точке доступа бита управления питанием в поле управления кадром, указывая, что станция перешла в режим работы с пониженным энергопотреблением. Оставшиеся три кадра (CF-подтверждение, CF-опрос, CF-подтверждение + CF-опрос) имеют те же функции, что и описанные выше подтипы кадров (данные + CF-подтверждение, данные + CF-опрос, данные + CF-подтверждение + CF-опрос), но не несут пользовательских данных.

Кадры управления

Кадры управления используются для управления связью станций и точек доступа. Возможны следующие подтипы:

- Запрос ассоциации. Посылается станцией к точке доступа с целью запроса ассоциации с данной сетью с базовым набором услуг (Basic Service Set - BSS). Кадр включает информацию о возможностях, например, будет ли использоваться шифрование, или способна ли станция отвечать при опросе.
- Ответ на запрос ассоциации. Возвращается точкой доступа и указывает, что запрос ассоциации принят.
- Запрос повторной ассоциации. Посылается станцией при переходе между BSS, когда требуется установить ассоциацию с точкой доступа в новом BSS. Использование повторной ассоциации, а не просто ассоциации, позволяет новой точке доступа договариваться со старой о передаче информационных кадров по новому адресу.
- Ответ на запрос повторной ассоциации. Возвращается точкой доступа и указывает, что запрос повторной ассоциации принят.
- Пробный запрос. Используется станцией для получения информации от другой станции или точки доступа. Кадр используется для локализации BSS стандарта IEEE 802.11.
- Ответ на пробный запрос. Отклик на пробный запрос.
- Сигнальный кадр. Передается периодически, позволяет мобильным станциям

локализовать и идентифицировать BSS.

- Объявление наличия трафика. Посылается мобильной станцией с целью уведомления других (которые могут находиться в режиме пониженного энергопотребления), что в буфере данной станции находятся кадры, адресованные другим.
- Разрыв ассоциации. Используется станцией для аннуляции ассоциации.
- Аутентификация. Для аутентификации станций используются множественные кадры.
- Отмена аутентификации. Передается для прекращения безопасного соединения.

Лекция 5. Стандарты IEEE 802.11

Из всех существующих стандартов беспроводной передачи данных IEEE 802.11 на практике чаще всего используются всего три стандарта, определенные Инженерным институтом электротехники и радиоэлектроники (IEEE): 802.11b, 802.11a и 802.11g.

В стандарте IEEE 802.11b благодаря высокой скорости передачи данных (до 11 Мбит/с), практически эквивалентной пропускной способности обычных проводных локальных сетей Ethernet, а также ориентации на диапазон 2,4 ГГц, этот стандарт завоевал наибольшую популярность у производителей оборудования для беспроводных сетей.

Поскольку оборудование, работающее на максимальной скорости 11 Мбит/с, имеет меньший радиус действия, чем на более низких скоростях, стандартом 802.11b предусмотрено автоматическое снижение скорости при ухудшении качества сигнала.

Стандарт IEEE 802.11a имеет большую ширину полосы из семейства стандартов 802.11 при скорости передачи данных до 54 Мбит/с.

В отличие от базового стандарта, ориентированного на область частот 2,4 ГГц, спецификациями 802.11a предусмотрена работа в диапазоне 5 ГГц. В качестве метода модуляции сигнала выбрано ортогональное частотное мультиплексирование (OFDM).

К недостаткам 802.11a относятся более высокая потребляемая мощность

радиопередатчиков для частот 5 ГГц, а также меньший радиус действия.

Стандарт IEEE 802.11g является логическим развитием 802.11b и предполагает передачу данных в том же частотном диапазоне. Кроме того, стандарт 802.11g полностью совместим с 802.11b, то есть любое устройство 802.11g должно поддерживать работу с устройствами 802.11b. Максимальная скорость передачи в стандарте 802.11g составляет 54 Мбит/с, поэтому на сегодня это наиболее перспективный стандарт беспроводной связи.

При разработке стандарта 802.11g рассматривались две отчасти конкурирующие технологии: метод ортогонального частотного разделения OFDM и метод двоичного пакетного сверточного кодирования PBCC, опционально реализованный в стандарте 802.11b. В результате стандарт 802.11g содержит компромиссное решение: в качестве базовых применяются технологии OFDM и CCK, а опционально предусмотрено использование технологии PBCC. О технологиях CCK и OFDM мы расскажем чуть позже.

Набор стандартов 802.11 определяет целый ряд технологий реализации физического уровня (Physical Layer Protocol - PHY), которые могут быть использованы подуровнем 802.11 MAC. В этой главе рассматривается каждый из уровней PHY:

- Уровень PHY стандарта 802.11 со скачкообразной перестройкой частоты (FHSS) в диапазоне 2,4 ГГц.
- Уровень PHY стандарта 802.11 с расширением спектра методом прямой последовательности (DSSS) в диапазоне 2,4 ГГц.
- Уровень PHY стандарта 802.11b с комплементарным кодированием в диапазоне 2,4 ГГц.
- Уровень PHY стандарта 802.11a с ортогональным частотным мультиплексированием (OFDM) в диапазоне 5 ГГц.
- Расширенный физический уровень (Extended Rate Physical Layer - ERP) стандарта 802.11g в диапазоне 2,4 ГГц.

Основное назначение физических уровней стандарта 802.11 - обеспечить механизмы беспроводной передачи для подуровня MAC, а также поддерживать выполнение вторичных функций, таких как оценка состояния беспроводной среды и сообщение о нем подуровню MAC. Уровни MAC и PHY разрабатывались так, чтобы они были независимыми. Именно независимость между MAC и подуровнем PHY и позволила использовать дополнительные высокоскоростные физические уровни, описанные в стандартах 802.11b, 802.11a и 802.11g.

Каждый из физических уровней стандарта 802.11 имеет два подуровня:

- Physical Layer Convergence Procedure (PLCP). Процедура определения состояния физического уровня.
- Physical Medium Dependent (PMD). Подуровень физического уровня, зависящий от среды передачи.

На рис. 3.1 показано, как эти подуровни соотносятся между собой и с вышестоящими уровнями в модели взаимодействия открытых систем (Open System Interconnection - OSI).

Подуровень PLCP по существу является уровнем обеспечения взаимодействия, на котором осуществляется перемещение элементов данных протокола MAC (MAC Protocol Data Units - MPDU) между MAC-станци-ями с использованием подуровня PMD, на котором реализуется тот или иной метод передачи и приема данных через беспроводную среду. Подуровни PLCP и PMD отличаются для разных вариантов стандарта 802.11.

Перед тем как приступить к изучению физических уровней, рассмотрим одну из составляющих физического уровня, до сих пор не упомянутую, а именно - скрэмблирование.

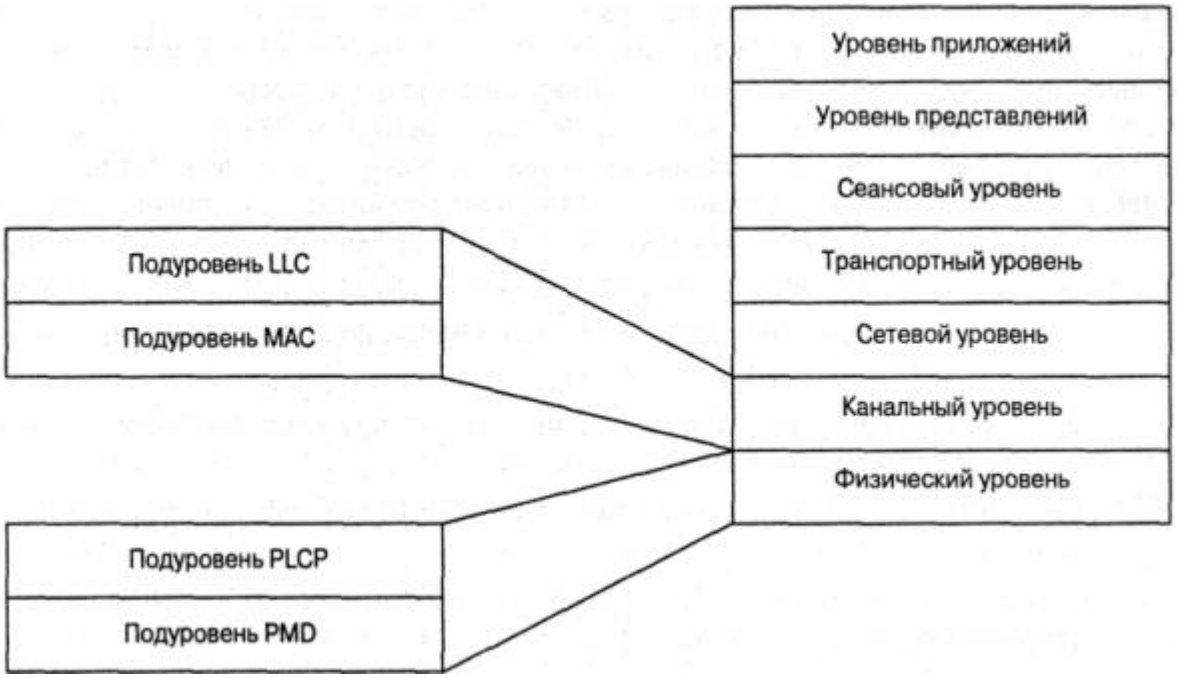


Рис. 3.1. Подуровни уровня PHY

Одна из особенностей, лежащих в основе современных передатчиков, благодаря которой данные можно передавать с высокой скоростью, - это предположение о том, что данные, которые предлагаются для передачи, поступают, с точки зрения передатчика, случайным образом. Без этого предположения многие преимущества, получаемые за счет применения остальных составляющих физического уровня, остались бы нереализованными.

Однако бывает, что принимаемые данные не вполне случайны и на самом деле могут содержать повторяющиеся наборы и длинные последовательности нулей и единиц.

Скрэмблирование (перестановка элементов) - это метод, посредством которого

принимаемые данные делаются более похожими на случайные; достигается это путем перестановки битов последовательности таким образом, чтобы превратить ее из структурированной в похожую на случайную. Эту процедуру иногда называют "отбеливанием потока данных". Де-скрэмблер приемника затем выполняет обратное преобразование этой случайной последовательности с целью получения исходной структурированной последовательности. Большинство способов скрэмблирования относится к числу самосинхронизирующихся; это означает, что дескрэмблер способен самостоятельно синхронизироваться со скрэмблером.

IEEE 802.11

Исходный стандарт 802.11 определяет три метода передачи на физическом уровне:

- Передача в диапазоне инфракрасных волн.
- Технология расширения спектра путем скачкообразной перестройки частоты (FHSS) в диапазоне 2,4 ГГц.
- Технология широкополосной модуляции с расширением спектра методом прямой последовательности (DSSS) в диапазоне 2,4 ГГц.

Передача в диапазоне инфракрасных волн

Средой передачи являются инфракрасные волны диапазона 850 нм, которые генерируются либо полупроводниковым лазерным диодом, либо светодиодом (LED). Так как инфракрасные волны не проникают через стены, область покрытия LAN ограничивается зоной прямой видимости. Стандарт предусматривает три варианта распространения излучения: ненаправленную антенну, отражение от потолка и фокусное направленное излучение. В первом случае узкий луч рассеивается с помощью системы линз. Фокусное направленное излучение предназначено для организации двухточечной связи, например между двумя зданиями.

Беспроводные локальные сети со скачкообразной перестройкой частоты (FHSS)

Беспроводные локальные сети FHSS поддерживают скорости передачи 1 и 2 Мбит/с. Устройства FHSS делят предназначенную для их работы полосу частот от 2,402 до 2,480 ГГц на 79 неперекрывающихся каналов (это справедливо для Северной Америки и большей части Европы). Ширина каждого из 79 каналов составляет 1 МГц, поэтому беспроводные локальные сети FHSS используют относительно высокую скорость передачи символов - 1 МГц - и намного меньшую скорость перестройки с канала на канал.

Последовательность перестройки частоты должна иметь следующие параметры: частота перескоков не менее 2,5 раз в секунду как минимум между шестью (6 МГц) каналами. Чтобы минимизировать число коллизий между перекрывающимися зонами покрытия, возможные последовательности перескоков должны быть

разбиты на три набора последовательностей, длина которых для Северной Америки и большей части Европы составляет 26. В таблице 3.1 представлены схемы скачкообразной перестройки частоты, обеспечивающие минимальное перекрытие.

По сути, схема скачкообразной перестройки частоты обеспечивает неторопливый переход с одного возможного канала на другой таким образом, что после каждого скачка покрывается полоса частот, равная как минимум 6 МГц, благодаря чему в многосотовых сетях минимизируется возможность возникновения коллизий.

Таблица 3.1. Схема FHSS для Северной Америки и Европы

Набор	Схема скачкообразной перестройки частоты
1	{0,3,6,9,12,15,18,21,24,27,30,33,36,39,42,45,48,51,54,57,60,63,66,69,72,75}
2	{1,4,7,10,13,16,19,22,25,28,31,34,37,40,43,46,49,52,55,58,61,64,67,70,73,76}
3	{2,5,8,11,14,17,20,23,26,29,32,35,38,41,44,47,50,53,56,59,62,65,68,71,72,77}

После того как уровень MAC пропускает MAC-фрейм, который в локальных беспроводных сетях FHSS называется также служебным элементом данных PLCP, или PSDU (PLCP Service Data Unit), подуровень PLCP добавляет два поля в начало фрейма, чтобы сформировать таким образом фрейм PPDU (PPDU - элемент данных протокола PLCP). На рис. 3.2 представлен формат фрейма FHSS подуровня PLCP.

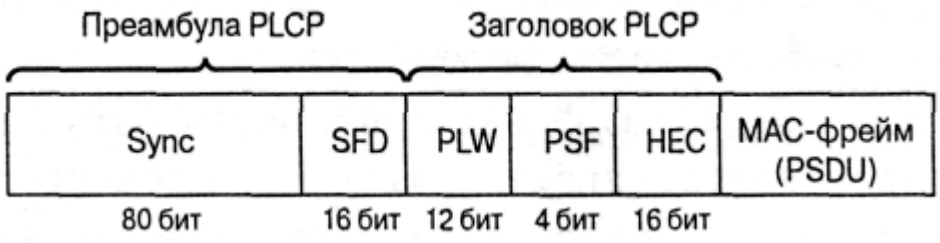


Рис. 3.2. Формат фрейма FHSS подуровня PLCP

Преамбула PLCP состоит из двух подполей:

- Подполе Sync размером 80 бит. Строка, состоящая из чередующихся 0 и 1, начинается с 0. Приемная станция использует это поле, чтобы принять решение о выборе антенны при наличии такой возможности, откорректировать уход частоты (frequency offset) и синхронизировать распределение пакетов (packet timing).

- Подполе флага начала фрейма (Start of Frame Delimiter, SFD) размером 16 бит. Состоит из специфической строки (0000 1100 1011 1101, крайний слева бит первый) в обеспечение синхронизации фреймов (frame timing) для приемной станции.

Заголовок фрейма PLCP состоит из трех подполей:

- Слово длины служебного элемента данных PLCP (PSDU), PSDU Length Word (PLW) размером 12 бит. Указывает размер фрейма MAC (PSDU) в октетах.
- Сигнальное поле PLCP (Signaling Field PLCP - PSF) размером 4 бит. Указывает скорость передачи данных конкретного фрейма.
- HEC (Header Error Check). Контрольная сумма фрейма.

Служебный элемент данных PLCP (PSDU) проходит через операцию скрэмблирования с целью отбеливания (рандомизации) последовательности входных битов. Получившийся в результате PSDU представлен на рис. 3.3. Заполняющие символы вставляются между всеми 32-сим-вольными блоками. Эти заполняющие символы устраняют любые систематические отклонения в данных, например, когда единиц больше, чем нулей, или наоборот, которые могли бы привести к нежелательным эффектам при дальнейшей обработке.

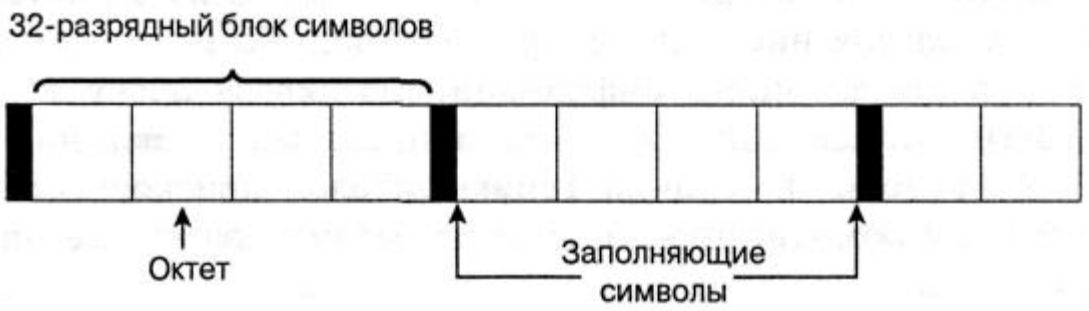


Рис. 3.3. Скрэмблированный PSDU в технологии FHSS

Подуровень PLCP преобразует фрейм в поток битов и передает его на подуровень PMD. Подуровень PMD технологии FHSS модулирует поток данных с использованием модуляции, основанной на гауссовой частотной модуляции (Gaussian Frequency Shift Keying - GFSK).

Беспроводные локальные сети, использующие широкополосную модуляцию DSSS с расширением спектра методом прямой последовательности

В спецификации стандарта 802.11 оговорено использование и другого физического уровня - на основе технологии широкополосной модуляции с расширением спектра методом прямой последовательности (DSSS). Как было указано в стандарте 802.11 разработки 1997 года, технология DSSS поддерживает скорости передачи 1 и 2 Мбит/с.

Аналогично подуровню PLCP, используемому в технологии FHSS, подуровень PLCP

технологии DSSS стандарта 802.11 добавляет два поля во фрейм MAC, чтобы сформировать PPDU: преамбулу PLCP и заголовок PLCP Формат фрейма представлен на рис. 3.4.

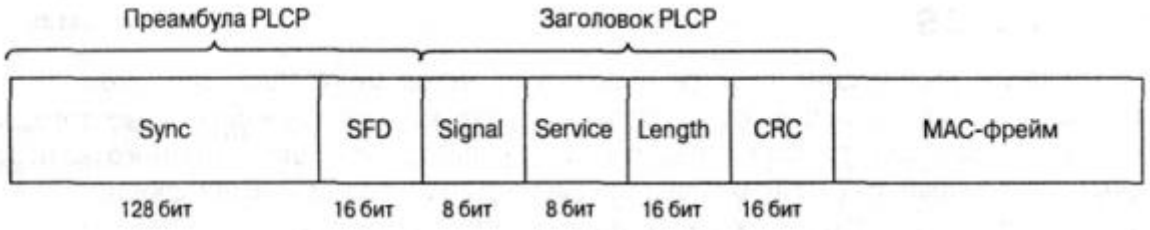


Рис. 3.4. Формат фрейма DSSS подуровня PLCP

Преамбула PLCP состоит из двух подполей:

- Подполе Sync шириной 128 бит, представляющее собой строку, состоящую из единиц. Задача этого подполя - обеспечить синхронизацию для приемной станции.
- Подполе SFD шириной 16 бит; в нем содержится специфичная строка OxF3A0; его задача - обеспечить тайминг (timing) для приемной станции.

Заголовок PLCP состоит из четырех подполей:

- Подполе Signal шириной 8 бит, указывающее тип модуляции и скорость передачи для данного фрейма.
- Подполе Service шириной 8 бит зарезервировано. Это означает, что во время разработки спецификации стандарта оно осталось неопределенным; предполагается, что оно пригодится в будущих модификациях стандарта.
- Подполе Length шириной 16 бит, указывающее количество микросекунд (из диапазона 16-216 _ 1), необходимое для передачи части MAC-фрейма.
- Подполе CRC. 16-битная контрольная сумма.

Подуровень PLCP преобразует фрейм в поток битов и передает данные на подуровень PMD. Весь PPDU проходит через процесс скрэмблирования с целью рандомизации данных.

Скрэмблированная преамбула PLCP всегда передается со скоростью 1 Мбит/с, в то время как скрэмблированный фрейм MPDU передается со скоростью, указанной в подполе Signal. Подуровень PMD модулирует отбеленный поток битов, используя следующие методы модуляции:

- Двоичная относительная фазовая модуляция (Differential Binary Phase Shift Keying - DBPSK) для скорости передачи 1 Мбит/с.
- Квадратурная относительная фазовая модуляция (Differential Quadrature Phase Shift Key - DQPSK) для скорости передачи 2 Мбит/с.

IEEE 802.11b

На физическом уровне к MAC-кадрам (MPDU) добавляется заголовок физического уровня, состоящий из преамбулы и собственно PLCP-заголовка (рис. 3.5).

Преамбула содержит стартовую синхропоследовательность (SYNC) для настройки приемника и 16-битный код начала кадра (SFD) - число F3A016. PLCP-заголовок включает поля SIGNAL (информация о скорости и типе модуляции), SERVICE (дополнительная информация, в том числе о применении высокоскоростных расширений и PBSS-модуляции) и LENGTH (время в микросекундах, необходимое для передачи следующей за заголовком части кадра). Все три поля заголовка защищены 16-битной контрольной суммой CRC.

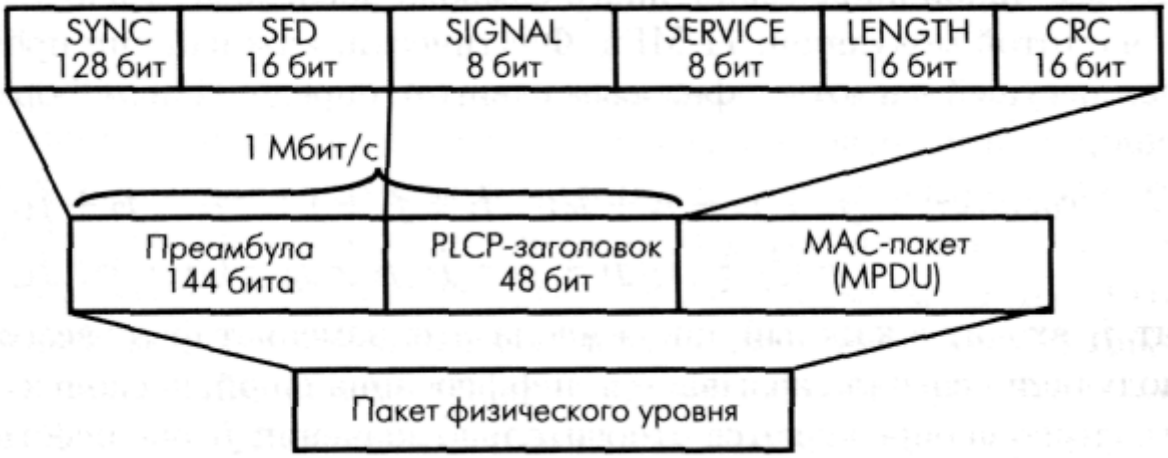


Рис. 3.5. Структура кадров сети IEEE 802.11b физического уровня

В стандарте IEEE 802.11b предусмотрено два типа заголовков: длинный и короткий (рис. 3.6).

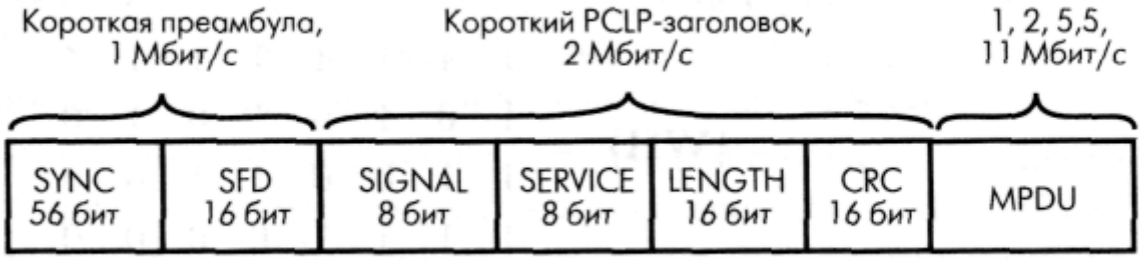


Рис. 3.6. Короткий заголовок кадров сети 802.11b

Они отличаются длиной синхропоследовательности (128 и 56 бит), способом ее генерации, а также тем, что символ начала кадра в коротком заголовке передается в обратном порядке. Кроме того, если все поля длинного заголовка передаются со скоростью 1 Мбит/с, то при коротком заголовке преамбула

транслируется на скорости 1 Мбит/с, другие поля заголовка - со скоростью 2 Мбит/с. Остальную часть кадра можно передавать на любой из допустимых стандартом скоростей передачи, указанных в полях SIGNAL и SERVICE. Короткие заголовки физического уровня предусмотрены спецификацией IEEE 802.11b для увеличения пропускной способности сети.

Из описания процедур связи сети IEEE 802.11 видно, что "накладные расходы" в этом стандарте выше, чем в проводной сети Ethernet. Поэтому крайне важно обеспечить высокую скорость передачи данных в канале. Повысить пропускную способность канала с заданной шириной полосы частот можно, разрабатывая и применяя новые методы модуляции. По этому пути пошла группа разработчиков IEEE 802.11b.

Напомним, что изначально стандарт IEEE 802.11 предусматривал работу в режиме DSSS с использованием так называемой Баркеровской последовательности (Barker) длиной 11 бит: B1 = (10110111000). Каждый информационный бит замещается своим произведением по модулю 2 (операция "исключающее ИЛИ") с данной последовательностью, т. е. каждая информационная единица заменяется на B1, каждый ноль - на инверсию B1. В результате бит заменяется последовательностью 11 чипов. Далее сигнал кодируется посредством дифференциальной двух- или четырехпози-ционной фазовой модуляции (DBPSK или DQPSK, один или два чипа на символ соответственно). При частоте модуляции несущей 11 МГц общая скорость составляет в зависимости от типа модуляции 1 и 2 Мбит/с.

Стандарт IEEE 802.11b дополнительно предусматривает скорости передачи 11 и 5,5 Мбит/с. Для этого используется так называемая ССК-модуляция (Complementary Code Keying - кодирование комплементарным кодом).

Хотя механизм расширения спектра, используемый для получения скоростей 5,5 и 11 Мбит/с с применением ССК, относится к методам, которые применяются для скоростей 1 и 2 Мбит/с, он по-своему уникален. В обоих случаях применяется метод расширения, но при использовании модуляции ССК расширяющий код представляет собой код из 8 комплексных чипов, в то время как при работе со скоростями 1 и 2 Мбит/с применяется 11-разрядный код. 8-чиповый код определяется или 4, или 8 битами - в зависимости от скорости передачи данных. Скорость передачи чипов составляет 11 Мчип/с, т.е. при 8 комплексных чипах на символ и 4 или 8 битов на символ можно добиться скорости передачи данных 5,5 и 11 Мбит/с.

Для того чтобы передавать данные со скоростью 5,5 Мбит/с, нужно сгруппировать скрэмблированный поток битов в символы по 4 бита (b0, b1, b2 и b3). Последние два бита (b2 и b3) используются для определения 8 последовательностей комплексных чипов, как показано в таблице 1.3, где {cl, c2, c3, c4, c5, c6, c7, c8} представляют чипы последовательности. В таблице 3.2 j представляет мнимое число, корень квадратный из -1, и откладывается по мнимой, или квадратурной, оси комплексной плоскости.

Таблица 3.2. Последовательность чипов ССК

(b2, b3)	C 1	C 2	C 3	C 4	C 5	C 6	C 7	C 8
00	j	1	j	-1	j	1	-1	1
01	-j	-1	-j	1	j	1	-j	1
10	-j	1	-j	-1	-j	1	j	1
11	j	-1	j	1	-j	1	j	1

Теперь, имея последовательность чипов, определенную битами (b2, b3), можно использовать первые два бита (b0, b1) для определения поворота фазы, осуществляемого при модуляции по методу DQPSK, который будет применен к последовательности (таблица 3.3). Вы должны также пронумеровать каждый 4-битовый символ PSDU, начиная с 0, чтобы можно было определить, преобразуете вы четный либо нечетный символ в соответствии с этой таблицей. Следует помнить, что речь идет об использовании DQPSK, а не QPSK, и поэтому представленные в таблице изменения фазы отсчитываются по отношению к предыдущему символу или, в случае первого символа PSDU, по отношению к последнему символу предыдущего DQPSK-символа, передаваемого со скоростью 2 Мбит/с.

Таблица 3.3. Поворот фазы при модуляции ССК

(b0, b1)	**Изменение фазы четных символов**	**Изменение фазы нечетных символов**
00	0	π
01	$\pi/2$	$-\pi/2$
11	π	0
10	$-\pi/2$	$\pi/2$

Это вращение фазы применяется по отношению к 8 комплексным чипам символа, затем осуществляется модуляция на подходящей несущей частоте.

Чтобы передавать данные со скоростью 11 Мбит/с, скрэмблированная последовательность битов PSDU разбивается на группы по 8 символов. Последние 6 битов выбирают одну последовательность, состоящую из 8 комплексных чипов, из числа 64 возможных последовательностей, почти так же, как использовались биты (b2, b3) для выбора одной из четырех возможных последовательностей. Биты (b0,b1) используются таким же образом, как при модуляции ССК на скорости 5,5 Мбит/с для вращения фазы последовательности и дальнейшей модуляции на подходящей несущей частоте.

В чем достоинство ССК-модуляции? Дело в том, что чипы символа определяются на основе последовательностей Уолша-Адамара. Последовательности Уолша-Адамара хорошо изучены, обладают отличными автокорреляционными свойствами. Что немаловажно, каждая такая последовательность мало коррелирует сама с собой при фазовом сдвиге - очень полезное свойство при борьбе с переотраженными сигналами. Нетрудно заметить, что теоретическое операционное усиление ССК-модуляции - 3 дБ (в два раза), поскольку без кодирования QPSK-модулированный с частотой 11 Мбит/с сигнал может транслировать 22 Мбит/с. Как видно, ССК-модуляция представляет собой вид блочного кода, а потому достаточно проста при аппаратной реализации. Совокупность этих свойств и обеспечила ССК место в стандарте IEEE 802.11b в качестве обязательного вида модуляции.

На практике важно не только операционное усиление. Существенную роль играет и равномерность распределения символов в фазовом пространстве - они должны как можно дальше отстоять друг от друга, чтобы минимизировать ошибки их детектирования. И с этой точки зрения ССК-модуляция не выглядит оптимальной, ее реальное операционное усиление не превышает 2 дБ. Поэтому изначально прорабатывался другой способ модуляции - пакетное бинарное сверточное кодирование PBCC (Packet Binary Convolutional Coding). Этот метод вошел в стандарт IEEE 802.11b как дополнительная (необязательная) опция. Механизм PBCC (рис. 3.7) позволяет добиваться в сетях IEEE 802.11b пропускной способности 5,5, 11 и 22 Мбит/с.

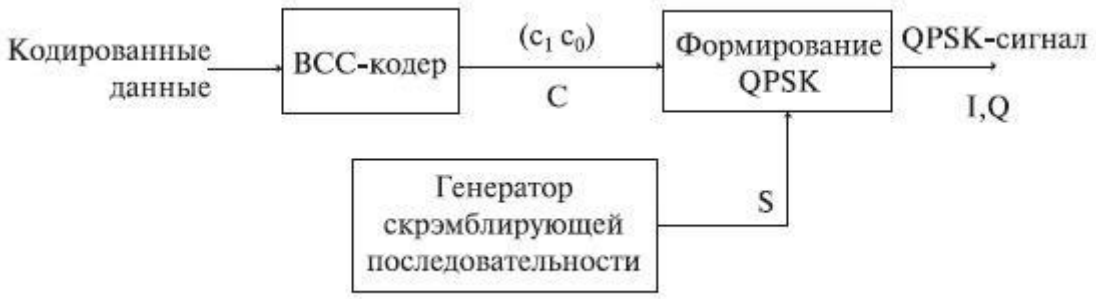


Рис. 3.7. Общая схема PBCC-модуляции

Как следует из названия, метод основан на сверточном кодировании. Для скоростей 5,5 и 11 Мбит/с поток информационных битов поступает в шестиразрядный сдвиговый регистр с сумматорами (рис. 3.8). В начальный момент времени все триггеры сдвигового регистра инициализируют нулем. В результате каждый исходный бит d заменяется двумя битами кодовой последовательности (c0, c1). При скорости 11 Мбит/с c0 и c1 задают один символ четырехпозиционной QPSK-модуляции. Для скорости 5,5 Мбит/с используют двухпозиционную BPSK-модуляцию, последовательно передавая кодовые биты c0 и c1. Если же нужна скорость 22 Мбит/с, схема кодирования усложняется (рис. 3.9): три кодовых бита (c0-c2) определяют один символ в 8-позиционной 8-PSK-модуляции.

После формирования PSK-символов происходит скрэмблирование. В зависимости от сигнала s (рис. 3.3) символ остается без изменений (s = 0), либо его фаза увеличивается на $\pi/2$ (s = 1). Значение s определяет 256-битовая циклически повторяющаяся последовательность S. Она формируется на основе начального вектора U = 338Bh, в котором равное число нулей и единиц.

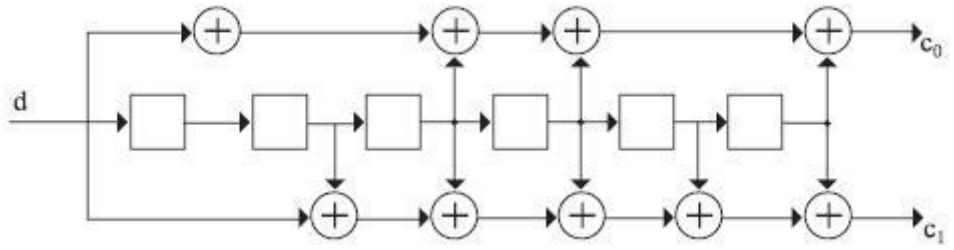


Рис. 3.8. Сверточное кодирование с двумя битами кодовой последовательности

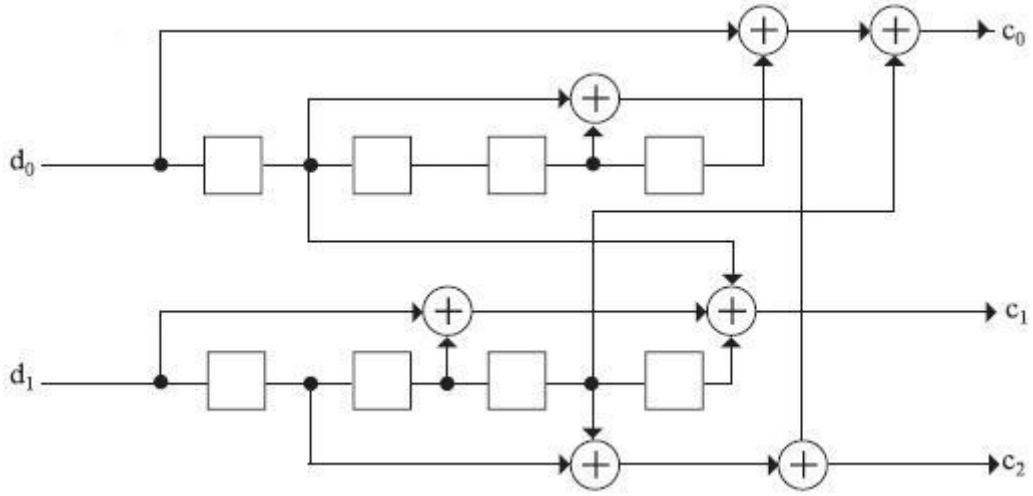


Рис. 3.9. Сверточное кодирование с тремя битами кодовой последовательности

У шестиразрядного сдвигового регистра, применяемого в PBCC для скоростей 11 и 5,5 Мбит/с, 64 возможных выходных состояния. Так что при модуляции PBCC информационные биты в фазовом пространстве оказываются гораздо дальше друг от друга, чем при CCK-модуляции. Поэтому PBCC и позволяет при одном и том же соотношении "сигнал-шум" и уровне ошибок вести передачу с большей скоростью, чем в случае CKK. Однако плата за более эффективное кодирование - сложность аппаратной реализации данного алгоритма.

IEEE 802.11a

Стандарт IEEE 802.11a появился практически одновременно с IEEE 802.11b, в сентябре 1999 года. Эта спецификация была ориентирована на работу в диапазоне 5 ГГц и основана на принципиально ином, чем описано выше, механизме кодирования данных - на частотном мультиплексировании посредством

ортогональных несущих (OFDM).

Стандарт 802.11a определяет характеристики оборудования, применяемого в офисных или городских условиях, когда распространение сигнала происходит по многолучевым каналам из-за множества отражений.

В IEEE 802.11a каждый кадр передается посредством 52 ортогональных несущих, каждая с шириной полосы порядка 300 КГц (20 МГц/64). Ширина одного канала - 20 МГц. Несущие модулируют посредством BPSK, QPSK, а также 16- и 64-позиционной квадратурной амплитудной модуляции (QAM). В совокупности с различными скоростями кодирования r (1/2 и 3/4, для 64-QAM - 2/3 и 3/4) образуется набор скоростей передачи 6, 9, 12, 18, 24, 36, 48 и 54 Мбит/с. В таблице 3.4 показано, как необходимая скорость передачи данных преобразуется в соответствующие параметры узлов передатчика OFDM.

Таблица 3.4. Параметры передатчика стандарта 802.11a

Скорость передачи данных (Мбит/с)	**Модуляция**	**Скорость сверточного кодирования**	**Число канальных битов на поднесущую**	**Число канальных битов на символ**	**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

Из 52 несущих 48 предназначены для передачи информационных символов, остальные 4 - служебные. Структура заголовков физического уровня отличается от принятого в спецификации IEEE 802.11b, но незначительно (рис. 3.10).

Рис. 3.10. Структура заголовка физического уровня стандарта IEEE 802.11a

Кадр включает преамбулу (12 символов синхропоследовательности), заголовок физического уровня (PLCP-заголовок) и собственно информационное поле, сформированное на MAC-уровне. В заголовке передается информация о скорости кодирования, типе модуляции и длине кадра. Преамбула и заголовок транслируются с минимально возможной скоростью (BPSK, скорость кодирования r = 1/2), а информационное поле - с указанной в заголовке, как правило, максимальной, скоростью, в зависимости от условий обмена. OFDM-символы передаются через каждые 4 мкс, причем каждому символу длительностью 3,2 мкс предшествует защитный интервал 0,8 мкс (повторяющаяся часть символа). Последний необходим для борьбы с многолучевым распространением сигнала - отраженный и пришедший с задержкой символ попадет в защитный интервал и не повредит следующий символ.

Естественно, формирование/декодирование OFDM-символов происходит посредством быстрого преобразования Фурье (обратного/прямого, ОБПФ/БПФ). Функциональная схема трактов приема/передачи (рис. 3.11) достаточно стандартна для данного метода и включает сверточный кодер, механизм перемежения/перераспределения (защита от пакетных ошибок) и процессор ОБПФ. Фурье-процессор, собственно, и формирует суммарный сигнал, после чего к символу добавляется защитный интервал, окончательно формируется OFDM-символ и посредством квадратурного модулятора/конвертера переносится в заданную частотную область. При приеме все происходит в обратном порядке.

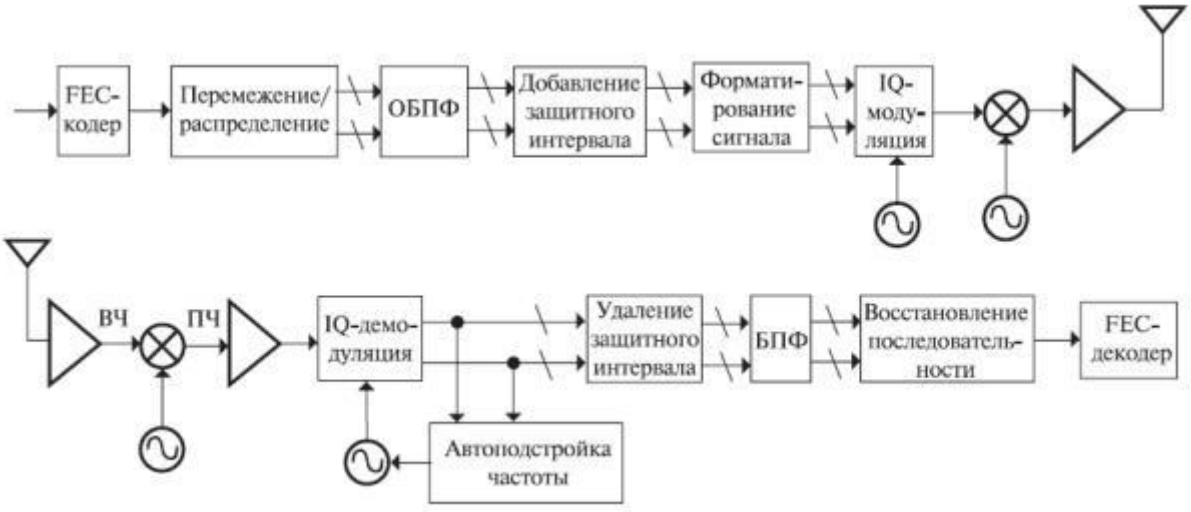


Рис. 3.11. Функциональная схема трактов приема/передачи стандарта IEEE 802.11a

IEEE 802.11g

Стандарт IEEE 802.11g по сути представляет собой перенесение схемы модуляции

OFDM, прекрасно зарекомендовавшей себя в 802.11a, из диапазона 5 ГГц в область 2,4 ГГц при сохранении функциональности устройств стандарта 802.11b. Это возможно, поскольку в стандартах 802.11 ширина одного канала в диапазонах 2,4 и 5 ГГц схожа - 22 МГц.

Одним из основных требований к спецификации 802.11g была обратная совместимость с устройствами 802.11b. Действительно, в стандарте 802.11b в качестве основного способа модуляции принята схема CCK (Complementary Code Keying), а в качестве дополнительной возможности допускается модуляция PBSS.

Разработчики 802.11g предусмотрели CCK-модуляцию для скоростей до 11 Мбит/с и OFDM для более высоких скоростей. Но сети стандарта 802.11 при работе используют принцип CSMA/CA - множественный доступ к каналу связи с контролем несущей и предотвращением коллизий. Ни одно устройство 802.11 не должно начинать передачу, пока не убедится, что эфир в его диапазоне свободен от других устройств. Если в зоне слышимости окажутся устройства 802.11b и 802.11g, причем обмен будет происходить между устройствами 802.11g посредством OFDM, то оборудование 802.11b просто не поймет, что другие устройства сети ведут передачу, и попытается начать трансляцию. Последствия очевидны.

Чтобы не допустить подобной ситуации, предусмотрена возможность работы в смешанном режиме - CCK-OFDM. Информация в сетях 802.11 передается кадрами. Каждый информационный кадр включает два основных поля: преамбулу с заголовком и информационное поле (рис. 3.12).

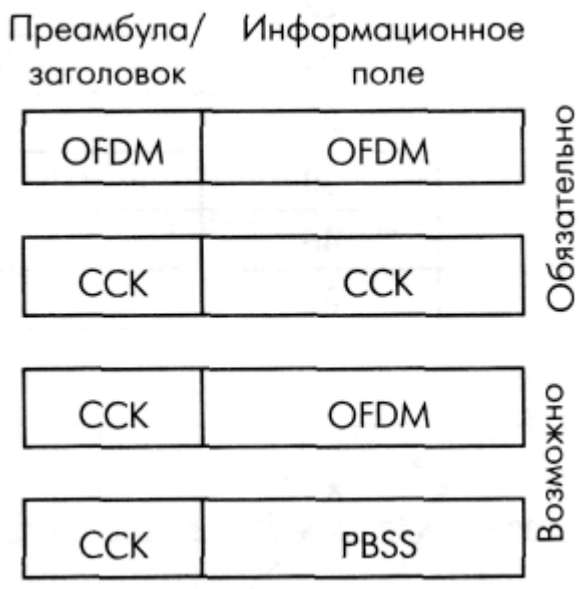


Рис. 3.12. Кадры IEEE 802.11g в различных режимах модуляции

Преамбула содержит синхропоследовательность и код начала кадра, заголовок - служебную информацию, в том числе о типе модуляции, скорости и продолжительности передачи кадра. В режиме CCK-OFDM преамбула и заголовок

модулируются методом CCK (реально - путем прямого расширения спектра DSSS посредством последовательности Баркера, поэтому в стандарте 802.11g этот режим именуется DSSS-OFDM), а информационное поле - методом OFDM. Таким образом, все устройства 802.11b, постоянно "прослушивающие" эфир, принимают заголовки кадров и узнают, сколько времени будет транслироваться кадр 802.11g. В этот период они "молчат". Естественно, пропускная способность сети падает, поскольку скорость передачи преамбулы и заголовка - 1 Мбит/с.

Видимо, данный подход не устраивал лагерь сторонников технологии PBSS, и для достижения компромисса в стандарт 802.11g в качестве дополнительной возможности ввели, так же как и в 802.11b, необязательный режим - PBSS, в котором заголовок и преамбула передаются так же, как и при CCK, а информационное поле модулируется по схеме PBSS и передается на скорости 22 или 33 Мбит/с. В результате устройства стандарта 802.11g должны оказаться совместимыми со всеми модификациями оборудования 802.11b и не создавать взаимных помех. Диапазон поддерживаемых им скоростей отражен в таблице 3.5, зависимость скорости от типа модуляции - на рис. 3.13.

Таблица 3.5. Возможные скорости и тип модуляции в спецификации IEEE 802.11g

Скорость, Мбит/с	**Тип модуляции**	
	Обязательно	**Допустимо**
1	Последовательность Баркера	
2	Последовательность Баркера	
5,5	CCK	PBCC
6	OFDM	OFDM
9		OFDM, CCK-OFDM
11	CCK	PBCC
12	OFDM	CCK-OFDM
18		OFDM, CCK-OFDM
22		PBCC
24	OFDM	CCK-OFDM
33		PBCC
36		OFDM, CCK-OFDM
48		OFDM, CCK-OFDM
54		OFDM, CCK-OFDM

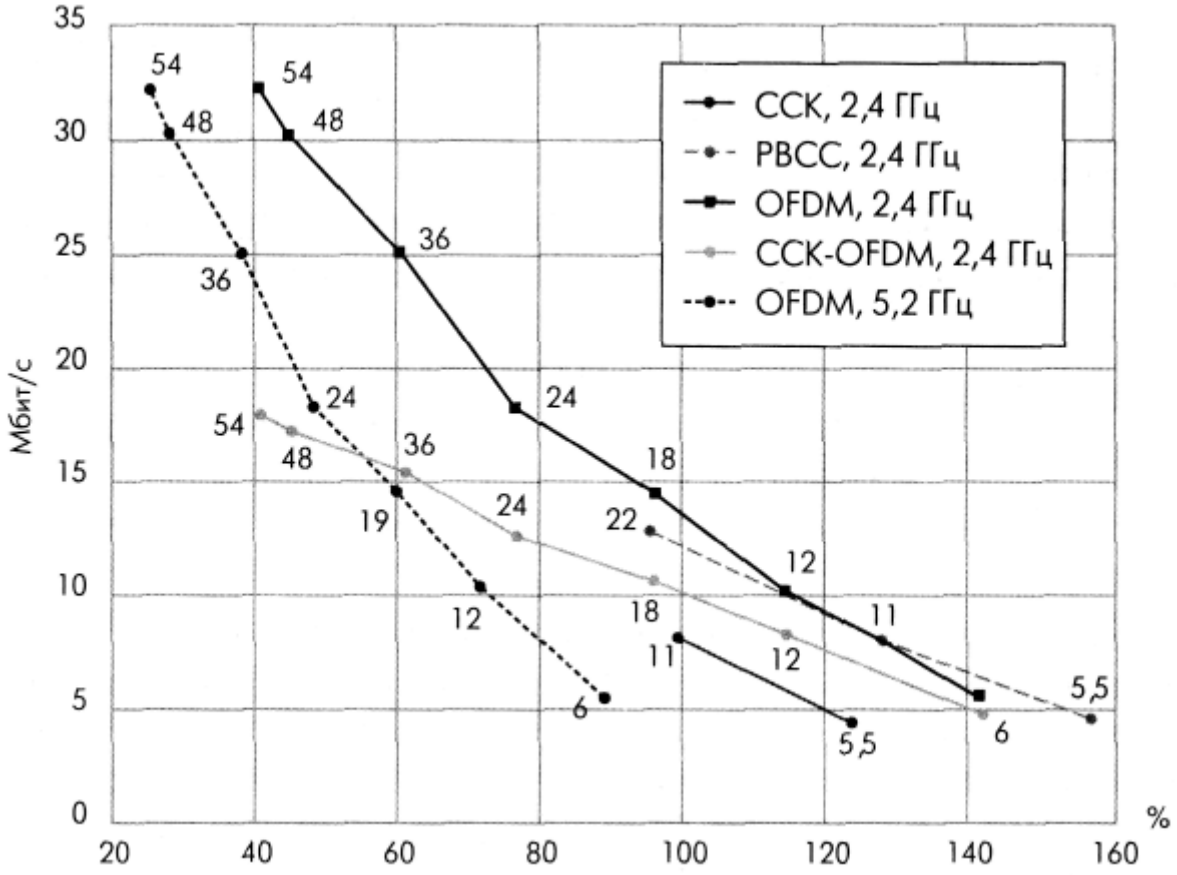


Рис. 3.13. Зависимость скорости передачи от расстояния для различных технологий передачи. Расстояние приведено в процентах, 100% - дальность передачи с модуляцией ССК на скорости 11 Мбит/с

Очевидно, что устройствам стандарта IEEE 802.11g достаточно долго придется работать в одних сетях с оборудованием 802.11b. Также очевидно, что производители в массе своей не будут поддерживать режимы CCK-OFDM и PBSS в силу их необязательности, ведь почти все решает цена устройства. Поэтому одна из основных проблем данного стандарта - как обеспечить бесконфликтную работу смешанных сетей 802.11b/g.

Основной принцип работы в сетях 802.11 - "слушать, прежде чем вещать". Но устройства 802.11b не способны услышать устройства 802.11g в OFDM-режиме. Ситуация аналогична проблеме скрытых станций: два устройства удалены настолько, что не слышат друг друга и пытаются обратиться к третьему, которое находится в зоне слышимости обоих. Для предотвращения конфликтов в подобной ситуации в 802.11 введен защитный механизм, предусматривающий перед началом информационного обмена передачу короткого кадра "запрос на передачу" (RTS) и получение кадра подтверждения "можно передавать" (CTS). Механизм RTS/CTS применим и к смешанным сетям 802.11b/g. Естественно, эти кадры должны транслироваться в режиме ССК, который обязаны понимать все устройства. Однако защитный механизм существенно снижает пропускную способность сети.

Стандарт 802.11n

для сетей Wi-Fi был утвержден организацией IEEE (Институт инженеров по электротехнике и радиоэлектронике) 11 сентября 2009 года.

В основе стандарта 802.11n:

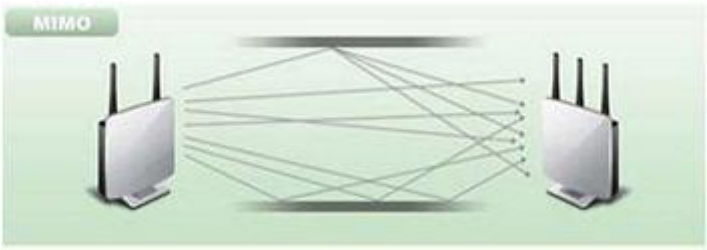
- *Увеличение скорости передачи данных;*
- *Увеличение зоны покрытия;*
- *Увеличение надежности передачи сигнала;*
- *Увеличение пропускной способности.*

Концепция 802.11n

Стандарт 802.11n включает в себя множество усовершенствований по сравнению с устройствами стандарта 802.11g.
Устройства 802.11n могут работать в одном из двух диапазонов 2.4 или 5.0 ГГц.
На физическом уровне (PHY) реализована усовершенствованная обработка сигнала и модуляции, добавлена возможность одновременной передачи сигнала через четыре антенны.
На сетевом уровне (MAC) реализовано более эффективное использование доступной пропускной способности. Вместе эти усовершенствования позволяют увеличить теоретическую скорость передачи данных до 600 Мбит/с – увеличение более чем в десять раз, по сравнению с 54 Мбит/с стандарта 802.11a/g (в настоящее время эти устройства уже считаются устаревшими).
В реальности, производительность беспроводной локальной сети зависит от многочисленных факторов, таких как среда передачи данных, частота радиоволн, размещение устройств и их конфигурация. При использовании устройств стандарта 802.11n, крайне важно понять, какие именно усовершенствования были реализованы в этом стандарте, на что они влияют, а также как они совмещаются и сосуществуют с сетями устаревшего стандарта 802.11a/b/g беспроводных сетей. Важно понять, какие именно дополнительные особенности стандарта 802.11n реализованы и поддерживаются в новых беспроводных устройствах.

Многоканальный вход/выход (MIMO)

Одним из основных моментов стандарта 802.11n является поддержка технологии MIMO (Multiple Input Multiple Output, Многоканальный вход/выход).
С помощью технологии MIMO реализована способность одновременного приема/передачи нескольких потоков данных через несколько антенн, вместо одной.



Чем больше устройство 802.11n использует антенн для одновременной работы передачи/приема, тем будет выше максимальная скорость передачи данных. Однако, само по себе использование нескольких антенн не увеличивает скорость передачи данных или расширение диапазона. Основным в устройствах стандарта 802.11n является то, что в них реализован усовершенствованный метод обработки сигнала, который и определяет алгоритм работы MIMO-устройства при использовании нескольких антенн.
При этом основное влияние на скорость оказывают широкие каналы и количество параллельных потоков данных (Spatial Streams). Так, передача с одним SS (S=1, в формуле MIMO T x R : S, где T - количество передающих антенн, R - количество принимающих антенн, S - количество SS) позволяет достичь скорости примерно 72.5Mbps при ширине канала 22Mhz и 150Mbps при ширине канала 40Mhz. Передача в два потока (TxR:2) - 145Mbps и 300Mbps соответственно. Три потока (TxR:3) - до 450Mbps на 40Mhz канале, и, соответственно, 600Mbps достигаются при четырех потоках и 40Mhz, что является максимумом для текущей версии спецификации 802.11n. При этом важно помнить, что для передачи N потоков необходимо иметь минимум N принимающих и N передающих антенн. Т.е. для двух SS допустимыми формулами MIMO могут быть и 2x2:2 (подавляющее большинство сегодняшних продуктов), и 2x3:2 (три принимающих антенны позволяют лучше работать в условиях переотражений), и 3x3:2 (High-end продукты). Для трех SS минимум уже 3x3:3, а для четырех, соответственно, 4x4:4. Все это удорожает продукт, **значительно** усложняет радиотракт и **серьезно** сказывается на потребляемой мощности.

Ширина полосы пропускания канала 40 МГц

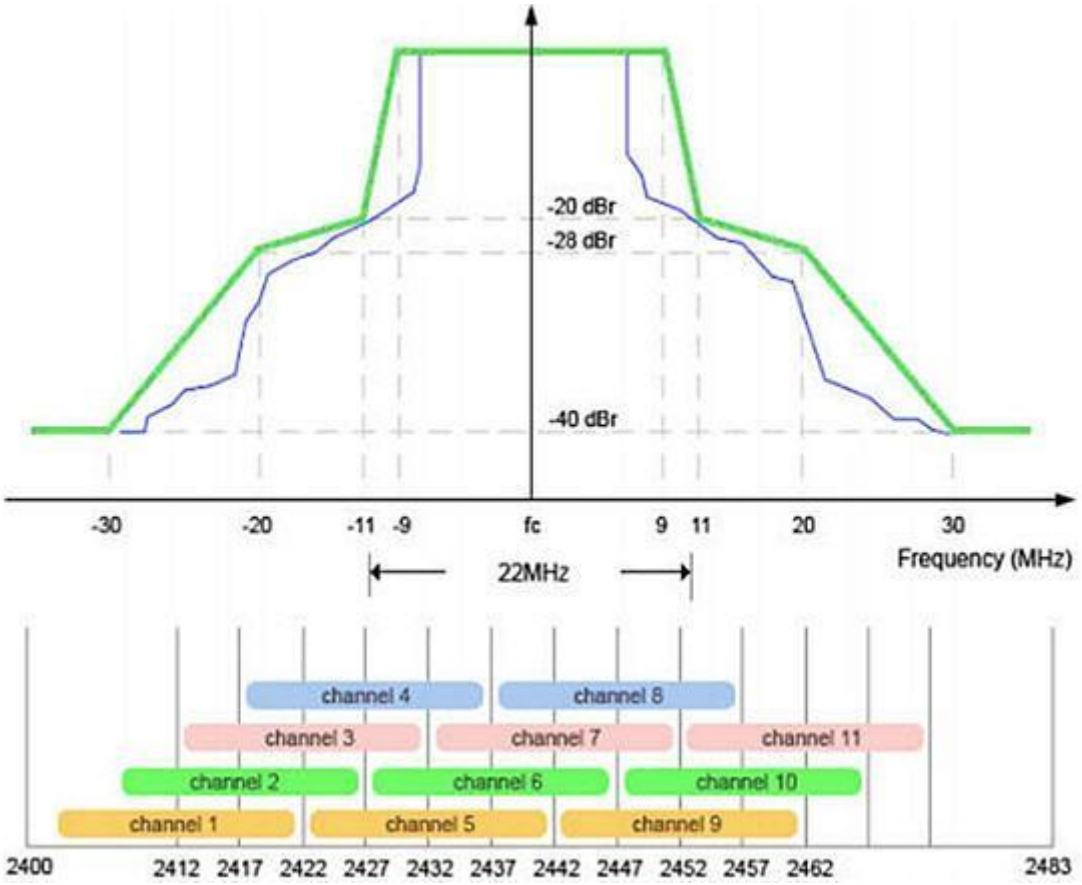
Другой дополнительной особенностью стандарта 802.11n является увеличение ширины канала с 20 до 40 МГц.

В беспроводных сетях используются два частотных диапазона 2.4 ГГц и 5 ГГц. Беспроводные сети стандарта 802.11b/g работают на частоте 2.4 ГГц, сети стандарта 802.11a работают на частоте 5 ГГц, а сети стандарта 802.11n могут работать как на частоте 2.4 ГГц, так и на частоте 5 ГГц.

В полосе частот 2.4 ГГц для беспроводных сетей доступны 13 каналов с интервалами 5 МГц между ними. Для передачи сигнала беспроводные устройства стандарта 802.11b/g используют каналы шириной 20 МГц. Беспроводное устройство стандарта 802.11b/g использует один из 13 каналов из полосы 20 МГц

в пределах частоты 2.4 ГГц, но фактически задействует 5 пересекающихся каналов. Например, если точка доступа использует канал 6, то она оказывает значительные помехи на каналы 5 и 7, а также оказывает помехи на каналы 4 и 8. Когда происходит передача данных устройством, беспроводной сигнал отклоняется от центральной частоты канала +/- 11 МГц. В некоторых случаях происходит отклонение энергии радиочастоты до 30 МГц от центрального канала. Для исключения взаимных помех между каналами необходимо, чтобы их полосы отстояли друг от друга на 25 МГц. Таким образом, остается всего 3 непересекающихся канала на полосе 20 МГц: 1, 6 и 11.

Беспроводные точки доступа, работающие в полосе частот 2.4 ГГц, в пределах одной покрываемой зоны обслуживания должны избегать перекрытия каналов для обеспечения качества беспроводной сети.



Одним из основных моментов является вопрос совместимости беспроводных устройств стандарта 802.11n с устройствами 802.11a/b/g.

Большинство беспроводных локальных сетей 802.11n используют каналы 40 МГц только в диапазоне частот 5 ГГц. В сетях, использующих полосу частот 5 ГГц (802.11n), проблемы пересекающихся каналов не существует.
Устройства стандарта 802.11n могут использовать ширину канала 20 или 40 МГц в любом частотном диапазоне (2.4 или 5 ГГц). При использовании ширины канала 40 МГц (устройства 802.11n) происходит двойное увеличение пропускной способности по сравнению с шириной канала 20 МГц (устройства 802.11b/g).
В полосе частот 5 ГГц доступно 19 непересекающихся каналов, которые более

пригодны для применения в устройствах стандарта 802.11n, обеспечивающих максимально возможную скорость передачи данных. Сигналы распределяются без взаимного перекрытия каналов с шириной полосы 40 МГц.

Однако, при использовании полосы 40 МГц устройствами 802.11n, их работе могут мешать существующие 802.11b/g точки доступа, что приведет к снижению производительности всего сегмента сети.

Режимы работы 802.11n

Существуют три режима работы 802.11n: HT, Non-HT и HT Mixed.

Рассмотрим более подробно каждый из режимов.

Режим с высокой пропускной способностью HT (High Throughput)

Точки доступа 802.11n используют режим High Throughput (HT), известный также как "чистый" режим (Greenfield-режим), который предполагает отсутствие поблизости (в зоне покрытия) работающих устройств 802.11b/g, использующих ту же полосу частот. Если же такие устройства существуют в зоне покрытия, то они не смогут общаться с точкой доступа 802.11n. Таким образом, в этом режиме разрешены к использованию только клиенты 802.11n, что позволит воспользоваться преимуществами повышенной скорости и увеличенной дальностью передачи данных, обеспечиваемыми стандартом 802.11n.

Режим с невысокой пропускной способностью Non-HT

Точка доступа 802.11n с использованием режима Non-HT (известный также как наследуемый режим), отправляет все кадры в формате 802.11b/g, чтобы устаревшие станции смогли понять их. В этом режиме точка доступа должна использовать ширину каналов 20 МГц и при этом не будет использовать преимущества стандарта 802.11n. Для обеспечения обратной совместимости все устройства должны поддерживать этот режим. Нужно учитывать, что точка доступа 802.11n с использованием режима Non-HT не будет обеспечивать высокую производительность. При использовании этого режима передача данных осуществляется со скоростью, поддерживаемой самым медленным устройством.

Смешанный режим с высокой пропускной способностью HT Mixed

Смешанный режим HT Mixed будет наиболее распространенным режимом для точек доступа 802.11n в ближайшие несколько лет. В этом режиме, усовершенствования стандарта 802.11n могут быть использованы одновременно с существующими станциями 802.11b/g. Режим HT Mixed обеспечит обратную совместимость устройств, но устройства 802.11n получат уменьшение пропускной способности. В этом режиме точка доступа 802.11n распознает наличие старых клиентов и будет использовать более низкую скорость передачи данных, пока старое устройство осуществляет прием-передачу данных.

Таким образом, при практическом применении улучшений стандарта 802.11n, преимущества могут быть достигнуты в полной мере только при условии, что клиенты 802.11b/g отсутствуют и беспроводная сеть работает в "чистом" режиме HT.

Индекс модуляции и схемы кодирования (MCS)

Точкам доступа и станциям 802.11n необходимо вести согласование пространственных потоков (Spatial Streams) и ширины канала. В зависимости от количества антенн возникают несколько пространственных потоков. Полную теоретически возможную пропускную способность стандарта 802.11n в 600 Мбит/с можно достичь лишь при использовании четырех передающих и четырех приемных антенн (конфигурация "4x4").
Стандарт 802.11n определяет Индекс модуляции и схемы кодирования MCS (Modulation and Coding Scheme). MCS - простое целое число, присваиваемое каждому варианту модуляции (всего возможно 77 вариантов). Каждый вариант определяет тип модуляции радиочастоты (Type), скорость кодирования (Coding Rate), защитный интервал (Short Guard Interval) и значения скорости передачи данных. Сочетание всех этих факторов определяет реальную физическую (PHY) скорость передачи данных, начиная от 6,5 Мбит/с до 600 Мбит/с (данная скорость может быть достигнута за счет использования всех возможных опций стандарта 802.11n).

Некоторые значения индекса MCS определенны и показаны в следующей таблице:

MCS Index	Type	Coding Rate	Spatial Streams	Data Rate (Mbps) with 20 MHz CH		Data Rate (Mbps) with 40 MHz CH	
				800 ns	400 ns (SGI)	800 ns	400 ns (SGI)
0	BPSK	1 / 2	1	6.50	7.20	13.50	15.00
1	QPSK	1 / 2	1	13.00	14.40	27.00	30.00
2	QPSK	3 / 4	1	19.50	21.70	40.50	45.00
3	16-QAM	1 / 2	1	26.00	28.90	54.00	60.00
4	16-QAM	3 / 4	1	39.00	43.30	81.00	90.00
5	64-QAM	2 / 3	1	52.00	57.80	108.00	120.00
6	64-QAM	3 / 4	1	58.50	65.00	121.50	135.00
7	64-QAM	5 / 6	1	65.00	72.20	135.00	150.00
8	BPSK	1 / 2	2	13.00	14.40	27.00	30.00
9	QPSK	1 / 2	2	26.00	28.90	54.00	60.00
10	QPSK	3 / 4	2	39.00	43.30	81.00	90.00
11	16-QAM	1 / 2	2	52.00	57.80	108.00	120.00
12	16-QAM	3 / 4	2	78.00	86.70	162.00	180.00
13	64-QAM	2 / 3	2	104.00	115.60	216.00	240.00
14	64-QAM	3 / 4	2	117.00	130.00	243.00	270.00
15	64-QAM	5 / 6	2	130.00	144.40	270.00	300.00
16	BPSK	1 / 2	3	19.50	21.70	40.50	45.00
...	...	...	...	...	...	...	...
31	64-QAM	5 / 6	4	260.00	288.90	540.00	600.00

Тип модуляции и скорость кодирования определяют, как данные будут передаваться в радиоэфир. Например, модуляция BPSK (Binary Phase Shift Keying) была включена в первоначальный стандарт 802.11, в то время как модуляция QAM (Quadrature Amplitude Modulation) была добавлена в 802.11a. Новые методы модуляции и кодирования, как правило, более эффективные и поддерживают

более высокие скорости передачи данных, но устаревшие методы и скорости все еще поддерживаются для обратной совместимости.

Для достижения максимальной скорости соединения 300 Мбит/с необходимо, чтобы и точка доступа и беспроводной адаптер поддерживали два пространственных потока (Spatial Streams) и удвоенную ширину канала 40 МГц. Исходя из полученной скорости соединения по приведенной выше таблице можно точно определить сколько потоков и какая ширина канала были задействованы. Так скорости соединения 65 или 130 Мбит/с говорят от том, что одно из устройств точка доступа или адаптер используют одинарную ширину канала 20 МГц.

Расшифруем значения некоторых параметров.

Короткий защитный интервал SGI (Short Guard Interval) определяет интервал времени между передаваемыми символами (наименьшая единица данных, передаваемых за один раз). Этот интервал помогает при приеме данных избежать задержки из-за межсимвольных помех Inter-Symbol Interference (ISI) и преодолеть эхо (отражение звуковых волн). В устройствах стандарта 802.11b/g используется защитный интервал 800 нс, а в устройствах 802.11n есть возможность использования паузы всего в 400 нс. Более короткие интервалы привели бы к большему вмешательству и снижению пропускной способности, в то время как большие интервалы могут привести к нежелательным простоям в беспроводной среде. Короткий защитный интервал (SGI) повышает скорость передачи данных на 11 процентов.

MCS значения от 0 до 31 определяют тип модуляции и схемы кодирования, которые будут использоваться для всех потоков. MCS значения с 32 по 77 описывают смешанные комбинации, которые могут быть использованы для модуляций от двух до четырех потоков.

Точки доступа 802.11n должны поддерживать MCS значения от 0 до 15, в то время как 802.11n станции должны поддерживать MCS значения от 0 до 7. Все другие значения MCS, в том числе связанные с каналами шириной 40 МГц, коротким защитным интервалом (SGI), являются опциональными. Определение значения MCS и SGI для всех ваших устройств 802.11n, является хорошим способом для определения набора скоростей передачи данных, которые могут быть использованы вашей беспроводной сетью.

Безопасность

Стандарт 802.11n использует те же меры безопасности 802.11i (WPA2), используемые ранее на устройствах стандарта 802.11a/g. VPN может быть использован для защиты кадров 802.11n, несмотря на то, что VPN-шлюзам необходима поддержка более высокой пропускной способности для обеспечения защиты.

Новая система предотвращения вторжений (IPS, Intrusion Prevention System) в

беспроводной сети работает также как и ранее и способна обнаруживать и реагировать на небезопасные (Rogue AP) точки доступа 802.11n. Обращаем ваше внимание, что возможно обнаружение устройств 802.11n, только работающих в режимах Non-HT или Mixed HT, но не в "чистом" режиме HT (Greenfield).

В таблице 3.6 представлена сводная информация по параметрам физических уровней.

Таблица 3.6. Стандарты физического уровня

Параметр	**802.11 DSSS**	**802.11 FHSS**	**802.11b**	**802.11a**	**802.11g**
Частотный диапазон (ГГц)	2,4	2,4	2,4	5	2,4
Максимальная скорость передачи данных (Мбит/с)	2	2	11	54	54
Технология	DSSS	FHSS	CCK	OFDM	OFDM
Тип модуляции (для максимальной скорости передачи)	QPSK	GFSK	QPSK	64-QAM	64-QAM
Число неперекрывающихся каналов	3	3	3	15	3

802.11ac

Принятие финальной версии спецификации 802.11ac состоялось в январе 2014 года

- Каналы шириной 80Mhz и 160Mhz, что позволяет моментально удвоить/учетверить результаты 802.11n.
- Максимальное число Spatial Streams увеличили до 8, что позволяет еще раз удвоить скорости по сравнению с n.
- Оптимизация модуляции и методов передачи пакетов позволяет выжать еще немного ресурса и добиться того, что высокие скорости будут доступны не только в радиусе 4м от точки доступа. 256-QAM, rate 3/4 and 5/6, added as optional modes (vs. 64-QAM, rate 5/6 maximum in 802.11n).
- **Beamforming** — возможность динамически менять диаграмму направленности антенн (что реально для антенной решетки из 8 элементов). В идеале, это обозначает, что зона покрытия точки доступа

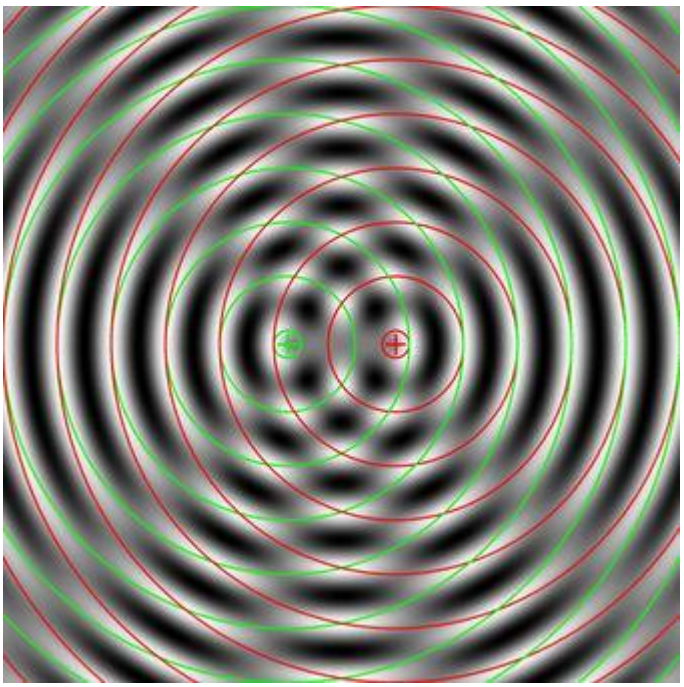
оптимально подстраивается под текущее расположение клиентов. Beamforming не нов для Wi-Fi, его даже сделали частью стандарта 802.11n. Но частью опциональной! В 802.11ac он станет частью обязательной. Пока неясно как именно будет работать Beamforming в 802.11ac и будет ли от него в итоге хоть какая-то польза, но совершенно очевидно, что вводится он для максимизации эффекта следующего *(и основного)* улучшения.

- **MU-MIMO** Сети Wi-Fi — полудуплексные: пока один передает — остальные слушают. Пакеты передаются последовательно — в один момент времени передается один пакет. Если по «трубе» в 450Mbps (802.11n 3x3:3 MIMO) идет поток в 1Mbps — используется 1/450 полосы пропускания. Если при этом прибывают данные для другого клиента — использовать незадействованную полосу пропускания не удастся. В итоге толку от сверхвысоких скоростей 802.11n в сетях с большим количеством небыстрых клиентов (т.е. корпоративных) очень мало. MU-MIMO позволяет разбить «трубу» на несколько «трубок меньшего диаметра» и передавать данные по ним параллельно. Эта технология хорошо известна телекомщикам. Пока что, говорят о двух вариантах реализации MU-MIMO в 802.11ac: SDMA (Space Division Multiple Access) позволяет передавать данные разным клиентам по разным Spatial Streams (вот где нужен Beamforming!), Downlink MIMO позволяет разбить поднесущие OFDM на группы, и динамически (вроде-бы) выделять каждому клиенту нужное число поднесущих. Таким образом, даже если на точке доступа будут сидеть клиенты 2x2:2 MIMO — все равно можно будет использовать весь потенциал «трубы».

  Фазированная антенная решётка — тип антенн, в виде группы антенных излучателей, в которых относительные фазы сигналов изменяются комплексно, так, что эффективное излучение антенны усиливается в каком-то одном, желаемом направлении и подавляется во всех остальных направлениях.

И снова о технологии формирования луча

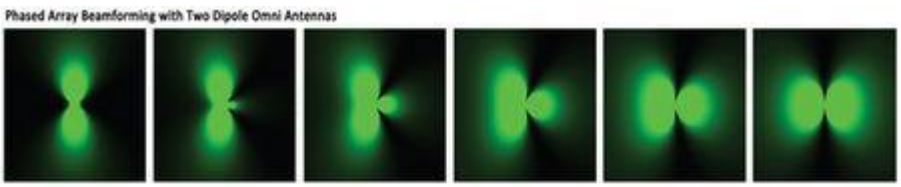
Целью технологии формирования луча является создание в определённом месте зоны с повышенной энергией волн. Классический пример этого явления: капли воды, падающие в бассейн. Если бы над ним были два крана и вы открывали каждый кран в точно определённый момент так, чтобы они время от времени выпускали синхронизированные по времени капли воды, концентрические волны-кольца, расходящиеся от каждого эпицентра (там, куда попадают капли), создали бы частично накладывающиеся друг на друга узоры. Вы видите такую модель на иллюстрации выше. Там, где волна оказывается в высшей точке пересечения с другой волной, вы получаете дополнительный эффект, при котором энергия обеих волн объединяется и ведёт к образованию ещё большего гребня в форме волны. Из-за регулярности падения капель такие усиленные гребни ясно видны в определённых направлениях, они составляют нечто вроде "луча" усиленной энергии.



В данном примере волны расходятся во всех направлениях. Они равномерно стремятся наружу от точки возникновения, пока не достигнут какой-либо противодействующий объект. Сигналы Wi-Fi, испускаемые с всенаправленной антенны, ведут себя таким же образом, выпуская волны радиочастотной энергии, которая, при объединении с волнами от другой антенны, может образовать лучи повышенного уровня сигнала. Когда в фазе у вас есть две волны, в результате может получиться луч с почти удвоенным уровнем сигнала, по сравнению с первоначальной волной.

Используемые во всех направлениях

Как видно из предыдушей фотографии уровня помех, формирование лучей с всенаправленных антенн происходит в многочисленных, часто противоположных, направлениях. Изменяя синхронизацию сигналов на каждой антенне, можно контролировать форму модели формирования луча. Это неплохо, потому что позволяет сфокусировать энергию в меньшем количестве направлений. Если бы ваша точка доступа "знала", что её клиент находится в положении на три часа, было ли бы разумным посылать луч на 9 или 11 часов? Ну, да... если присутствие этого "потерянного" луча неизбежно.

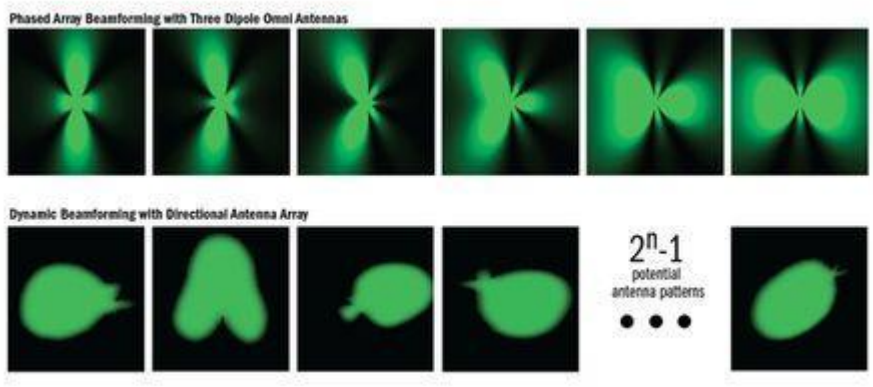


На самом деле, если имеешь дело с всесторонне направленными антеннами, то подобная потеря действительно неизбежна. Говоря техническим языком, то, что вы видите в верхнем ряду, – это результат действия фазированной антенной

решётки (ФАР) – группы антенн, в которой относительные фазы соответствующих сигналов, питающих антенны, различаются таким образом, что модель эффективного излучения решётки усиливается в требуемом направлении и подавляется в нескольких нежелательных направлениях. Это похоже на сжатие средней части не полностью надутого воздушного шара. При усилении сжатия получим часть шарика, чрезмерно выдающуюся в каком-то одном направлении, но также мы столкнёмся с соответствующим выбросом и в другом направлении. Вы можете это увидеть на рисунке выше, где верхний ряд показывает различные модели формирования луча, образованные двумя дипольными всенаправленными антеннами.

Внесение изменений в ходе формирования луча

Очевидно вы хотите, чтобы формируемая зона покрытия луча захватывала клиентское устройство. При формировании луча фазированной антенной решёткой, как проиллюстрировано на рисунках выше, в верхних строчках (на этот раз взяты три дипольных антенны), точка доступа анализирует сигналы, исходящие от клиента, и использует алгоритмы для изменения модели излучения, таким образом меняется направление прохождения луча для лучшего нацеливания на клиента. Данные алгоритмы высчитываются в контроллере точки доступа, вот почему иногда можно увидеть другое название этого процесса – "chip-based beamforming". Эта технология также широко известна под именем направленной передачи сигнала у Cisco и других компаний, и она остаётся дополнительным, не имеющим широкого распространения, компонентом спецификации 802.11n.



Фазированная антенная решётка с аппаратным управлением – это метод, используемый большинством производителей, которые в настоящее время широко рекламируют поддержку технологии формирования луча в своих товарах. Компания Ruckus не пользуется таким методом. В этом отношении, мы ошиблись в нашей предыдущей статье. На шестой странице наш автор утверждал, что "Ruckus использует метод формирования луча "на антенне" - технологию, разработанную и запатентованную Ruckus ... [при которой] применяется антенная решётка". Но это не тот случай. Формирование луча фазированной антенной решёткой требует

использования большого количества антенн. Подход Ruckus отличается от этого метода.

По технологии Ruckus можно направлять луч на каждую антенну, независимо от других антенн. Это достигается путём намеренного размещения металлических объектов поблизости от каждой антенны в антенной решётке, чтобы самостоятельно влиять на модель излучения. Вскоре мы вернёмся к этому вопросу и постараемся более основательно его изучить, но несколько разных типов моделей формирования луча с применением подхода Ruckus вы можете увидеть во втором ряду на рисунках выше. Глядя на оба подхода одновременно нельзя определить, какой из них даст самую высокую практическую производительность. Фазированная решётка из трёх антенн формирует более сфокусированный луч, чем блоки относительного покрытия от Ruckus. Интуитивно мы можем предположить, что чем больше сфокусирован луч, тем выше производительность, если все остальные факторы равны.

На рынок технология 802.11ac выходит несколькими этапами, названных "волнами".

- **Wave 1** позволяет пробиться за гигабитный барьер «сырой» скорости передачи данных (~1300 теоретических Mbps при 3x3:3 MIMO с шириной канала 80MHz и новой модуляцией 256-QAM). В целом, тот же 802.11n, но быстрее.
- **Wave 2** принесет дальнейшие улучшения в плане скорости (4x4:4 MIMO/160MHz ~= 3500Mbps) и емкости – MU-MIMO.
- **Последующие волны** могут принести остальные нововведения, считающиеся опциональными или слишком сложными для быстрого внедрения (типа 8x8:8 MIMO). А могут и не принести вообще — немало технологий описанных в стандарте 802.11n так и не были реализованы в реальных продуктах.

Возросшая скорость передачи. Тут всё понятно – сеть быстрее, все как бы рады. Только нужно помнить, что необходима поддержка на клиенте. Давайте посмотрим, что нужно для «пробития гигабитного барьера» на оборудовании Wave1. Дабы далеко не ходить, обратимся к табличке скоростей из Wikipedia

- При ширине канала **20MHz**, максимальная скорость на поток составляет **~87Mbps**, что означает, что при нынешнем ограничении в 3 потока, гигабита нам не видать.
- При ширине канала **40MHz**, максимальная скорость на поток составляет **~200Mbps**, что означает, что при нынешнем ограничении в 3 потока, гигабита нам не видать. Зато, по сравнению с 802.11n мы ускорились на треть (600/450) просто путем замены железа.
- При ширине канала **80MHz**, максимальная скорость на поток составляет **~433Mbps**, что означает, что нам нужно задействовать все 3 потока. Это накладывает довольно строгие требования на план покрытия: нужно обеспечить 80MHz-каналы (неперекрывающиеся для соседних ячеек, так что нам нужно минимум 4, а где их найти?), плюс, нужно обеспечить

благоприятную среду для трёх пространственных потоков, что не очень просто.

Даже с каналами 80MHz и правильным размещением точек, не стоит рассчитывать на гигабитные скорости. Большинство компактных клиентов не будет поддерживать три потока. Смартфоны обычно поддерживают 1 поток, планшеты – 1-2 потока, ноутбуки – 2-3 потока. Это важно помнить при планировании сети и не гнаться за скоростями, которые клиенты просто не смогут поддерживать. С Wave2 и MU-MIMO, однако, «малопоточные» клиенты будут обрабатываться гораздо эффективней. Скажем, точка с 4SS сможет параллельно вести передачу на 4 клиента с 1SS (по потоку на каждого) или на три клиента в комбинации 1+2+1 и т.д. Это должно значительно повысить эффективность использования эфирного времени и поднять емкость сети. Об этом ниже.

Возросшая чувствительность радио. Новые чипсеты (и на точках и на клиентах) обладают лучшей чувствительностью, поэтому считается, что для успешной работы 256-QAM (и достижения более высоких скоростей) не понадобится увеличивать плотность покрытия. Обратите внимание, что это никаким образом не относится к MIMO, да и уповать на порядочность производителей сверхдешевых клиентских устройств тоже не стоит.

Немаловажным нюансом является также **проводное подключение точек**. Точка 802.11n может «выжать» максимум 900Mbps из двух радио (3x3:3/40Mhz), для чего вполне достаточно одного линка GE. Точка 802.11ac Wave 1 теоретически может выжать 2x1300Mbps = 2.6Gbps, для чего не хватит даже трех линков GE (а Wave2 так вообще все 7Gbps). Апгрейдить всё на 10GE? Будет довольно дорого. К счастью (как минимум для Wave 1) этого не нужно. Важно помнить, что пропускная способность Ethernet исторически меряется с учетом оверхеда самого протокола («нетто»), а для Wi-Fi – без («брутто»). Так что теоретические «сырые» 2600Mbps вполне реально втиснуть в 2 линка GE. Большинство объявленных точек 802.11ac Wave 1 имеют 2 порта GE и считается что этого хватит. Правда, придется доплатить за дополнительные порты на свитчах и прокладку второго кабеля (обычно ~50% от стоимости прокладки первого). Опять же, если мы строим сеть для BYOD (т.е. клиенты будут поддерживать 1-2 потока), то может хватить и одного гигабита.

Возросшая емкость сети. Полезным побочным эффектом возросшей скорости является то, что передача того же объема данных занимает меньше времени :) Таким образом, возрастает емкость нашей полудуплексной ячейки. Предположим, у нас есть некоторое количество клиентов 802.11n 1x1:1/40MHz (150Mbps) на точке доступа, каждому из которых требуется 10Mbps полосы пропускания. Для удобства вычислений положим, что эффективная пропускная способность ячейки составит 0.6 от теоретической = 90Mbps. При полудуплексном обмене, таким образом, ячейка сможет поддерживать 9 клиентов. При апгрейде на 802.11ac, сохраняя ширину канала и количество потоков, мы сможем получить

теоретические 200Mbps в ячейке за счет 256-QAM, подняв емкость до 200*0.6/10 = 12 клиентов. Налицо прирост в 30% просто за счет замены железа. Если задуматься, кстати, емкость ячейки не зависит то того, будет ли у вас точка 2x2:2 или 3x3:3, т.к. при полудуплексной передаче для клиента 1x1:1 остальные потоки не используются. А вот с Wave2 и MU-MIMO в том же сценарии мы можем 12 клиентов легко превратить в 36 или 48. А при 8x8:8 — вообще в 96!

В принципе, вот и все основные факторы.

- С одной стороны: возросшая скорость и емкость
- С другой стороны: не всегда скорость достигается, требуется замена клиентов и точек (и те и те будут дороже), требуется апгрейд проводной части, всё купленное придется менять снова при выходе Wave2.

Лекция 6. Режимы и особенности их организации

Беспроводные сети Wi-Fi поддерживают несколько различных режимов работы, реализуемых для конкретных целей. Каждый режим сопровождается пояснительным рисунком для лучшего представления взаимодействия элементов сети. Большим плюсом является подробное описание настройки подключения, используя как встроенные в Windows службы, так и утилиту D-Link AirPlus XtremeG Wreless Utility, которая идет в комплекте с оборудованием D-Link. Очень интересно будет ознакомиться с режимами WDS и WDS WITH AP, которые образуют мостовое соединение. Для лекции характерно большое количество примеров установки, настройки и проверки соединения.

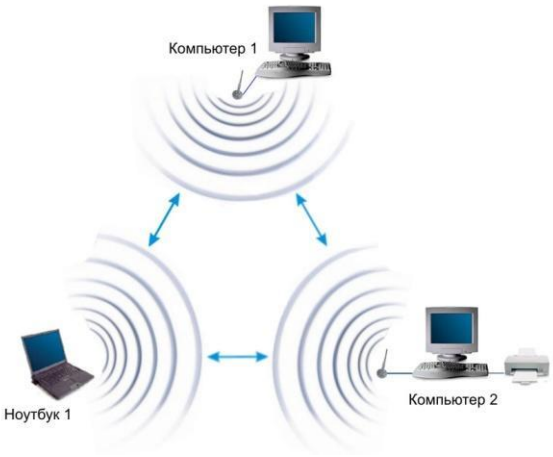
Режим Ad Hoc

В режиме Ad Hoc клиенты устанавливают связь непосредственно друг с другом. Устанавливается одноранговое взаимодействие по типу "точка-точка", и компьютеры взаимодействуют напрямую без применения точек доступа. При этом создается только одна зона обслуживания, не имеющая интерфейса для подключения к проводной локальной сети.

Основное достоинство данного режима - простота организации: он не требует дополнительного оборудования (точки доступа). Режим может применяться для создания временных сетей для передачи данных.

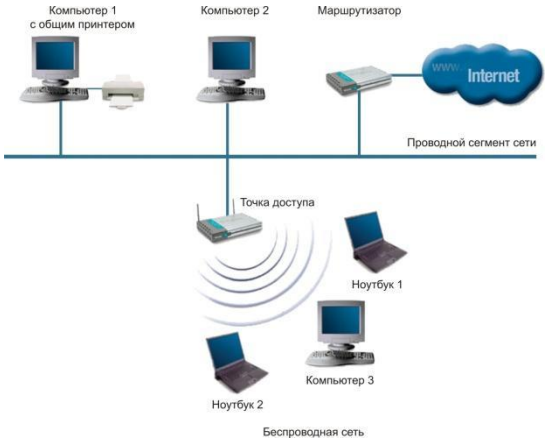
Однако необходимо иметь в виду, что режим Ad Hoc позволяет устанавливать соединение на скорости не более 11 Мбит/с, независимо от используемого оборудования. Реальная скорость обмена данными будет ниже и составит не более 11/N Мбит/с, где N - число устройств в сети. Дальность связи составляет не

более ста метров, а скорость передачи данных быстро падает с увеличением расстояния.



Инфраструктурный режим

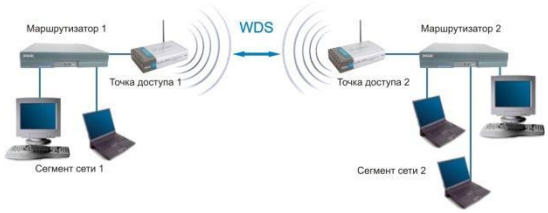
В этом режиме точки доступа обеспечивают связь клиентских компьютеров. Точку доступа можно рассматривать как беспроводной коммутатор. Клиентские станции не связываются непосредственно одна с другой, а связываются с точкой доступа, и она уже направляет пакеты адресатам.



Режимы WDS и WDS WITH AP

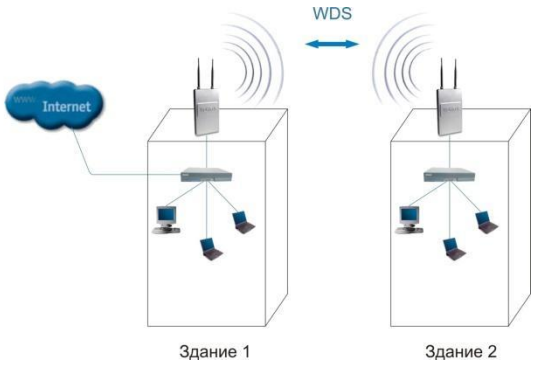
Термин WDS (Wireless Distribution System) расшифровывается как "распределенная беспроводная система". В этом режиме точки доступа соединяются только между собой, образуя мостовое соединение. При этом каждая точка может соединяться с несколькими другими точками. Все точки в этом режиме должны использовать

один и тот же канал, поэтому количество точек, участвующих в образовании моста, не должно быть чрезмерно большим. Подключение клиентов осуществляется только по проводной сети через uplink-порты точек.



Мостовой режим

Режим беспроводного моста, аналогично проводным мостам, служит для объединения подсетей в общую сеть. С помощью беспроводных мостов можно объединять проводные LAN, находящиеся как в соседних зданиях, так и на расстоянии до нескольких километров. Это позволяет объединить в сеть филиалы и центральный офис, а также подключать клиентов к сети провайдера Internet.



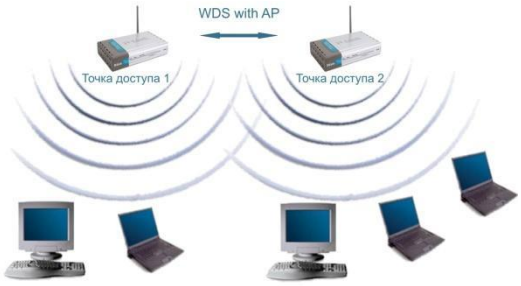
Мостовой режим между зданиями

Беспроводной мост может использоваться там, где прокладка кабеля между зданиями нежелательна или невозможна. Данное решение позволяет достичь значительной экономии средств и обеспечивает простоту настройки и гибкость конфигурации при перемещении офисов.

К точке доступа, работающей в режиме моста, подключение беспроводных

клиентов невозможно. Беспроводная связь осуществляется только между парой точек, реализующих мост.

Термин WDS with AP (WDS with Access Point) означает "распределенная беспроводная система, включающая точку доступа", т.е. с помощью этого режима можно не только организовать мостовую связь между точками доступа, но и одновременно подключить клиентские компьютеры. Это позволяет достичь существенной экономии оборудования и упростить топологию сети. Данная технология поддерживается большинством современных точек доступа.



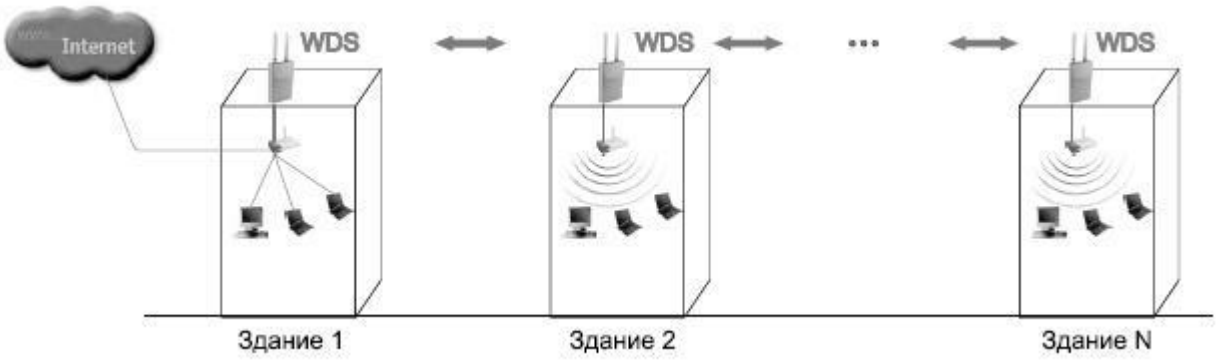
Режим WDS with AP

Тем не менее необходимо помнить, что все устройства в составе одной WDS with AP работают на одной частоте и создают взаимные помехи, что ограничивает количество клиентов до 15-20 узлов. Для увеличения количества подключаемых клиентов можно использовать несколько WDS-сетей, настроенных на разные неперекрывающиеся каналы и соединенные проводами через uplink-порты.

Топология организации беспроводных сетей в режиме WDS аналогична обычным проводным топологиям.

Топология типа "шина"

Топология типа "шина" самой своей структурой предполагает идентичность сетевого оборудования компьютеров, а также равноправие всех абонентов.



Топология типа "шина"

Здесь отсутствует центральный абонент, через которого передается вся информация, что увеличивает ее надежность (ведь при отказе любого центра перестает функционировать вся управляемая этим центром система). Добавить новых абонентов в шину довольно просто. Надо ввести параметры новой точки доступа, что приведет только к кратковременной перезагрузке последней точки.

Шине не страшны отказы отдельных точек, так как все остальные компьютеры сети могут нормально продолжать обмен между собой, но при этом оставшаяся часть компьютеров не сможет получить доступ в Internet.

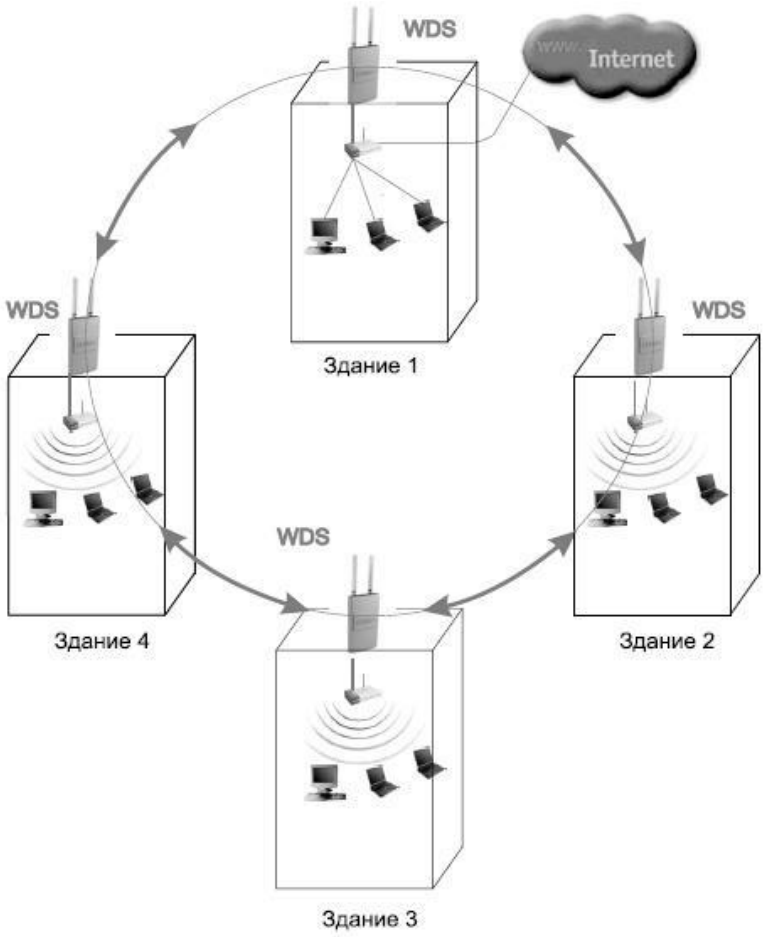
Топология типа "кольцо"

"Кольцо" - это топология, в которой каждая точка доступа соединена только с двумя другими. Четко выделенного центра в данном случае нет, все точки могут быть одинаковыми.

Подключение новых абонентов в "кольцо" обычно осуществить очень просто, хотя это и требует обязательной остановки работы двух крайних точек от новой точки доступа. В то же время основное преимущество кольца состоит в том, что ретрансляция сигналов каждым абонентом позволяет существенно увеличить размеры всей сети в целом (порой до нескольких десятков километров). Кольцо в этом отношении существенно превосходит любые другие топологии.

Топология связей между точками в этом режиме представляет собой ациклический граф типа "дерево", то есть данные из Internet от точки 4 к точке 2 проходят по двум направлениям - через точку 1 и 3 (рис. 4.15). Для устранения лишних связей, способных приводить к появлению циклов в графе, реализуется алгоритм Spanning tree. Его использование позволяет выявить и блокировать лишние связи. При изменении топологии сети - например, из-за отключения некоторых точек или невозможности работы каналов - алгоритм Spanning tree запускается заново, и

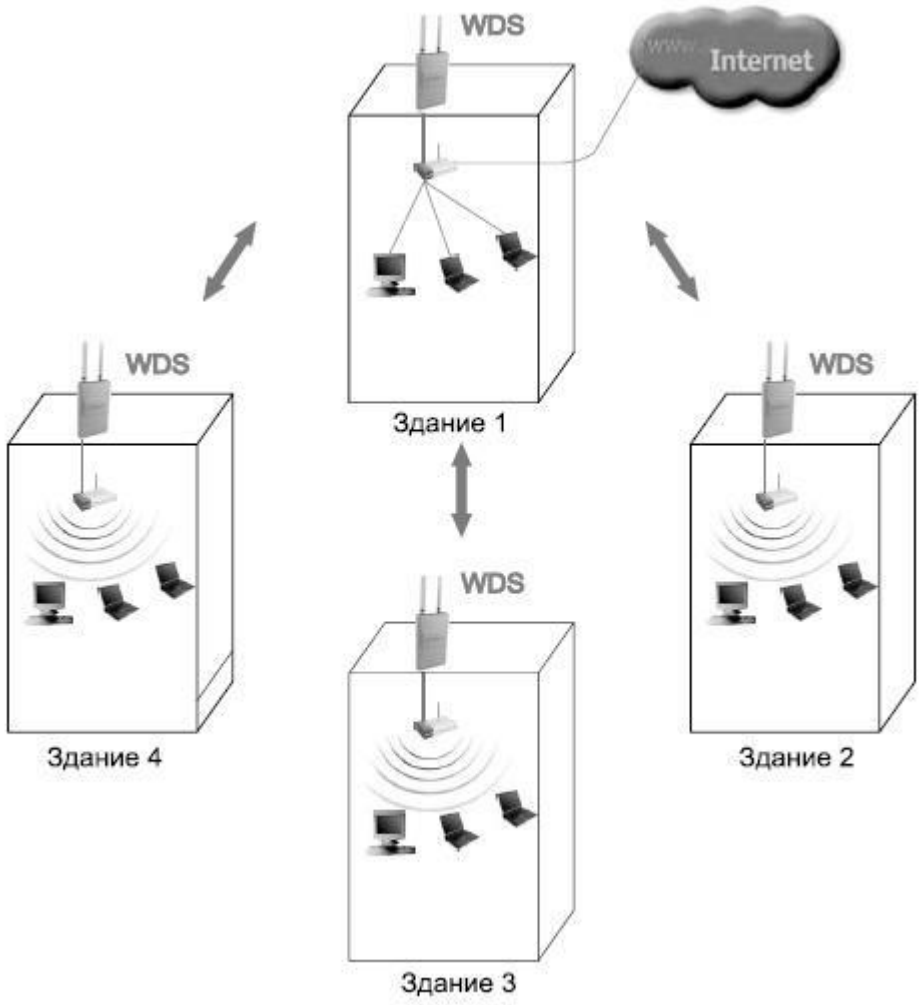
прежде заблокированные лишние связи могут использоваться вместо вышедших из строя.



Топология типа "звезда"

"Звезда" - это топология с явно выделенным центром, к которому подключаются все остальные абоненты. Весь обмен информацией идет исключительно через центральную точку доступа, на которую в результате ложится очень большая нагрузка.

Если говорить об устойчивости звезды к отказам точек, то выход из строя обычной точки доступа никак не отражается на функционировании оставшейся части сети, зато любой отказ центральной точки делает сеть полностью неработоспособной.



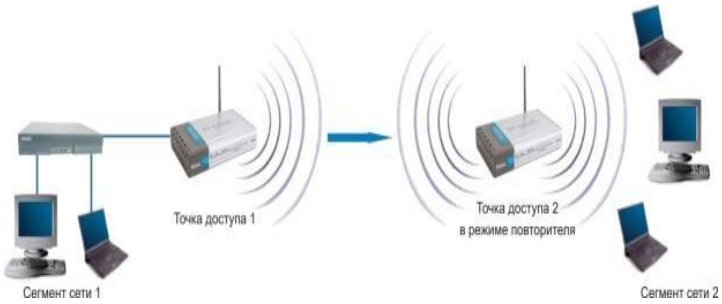
Топология типа "звезда"

Существенный недостаток топологии "звезда" состоит в жестком ограничении количества абонентов. Так как все точки работают на одном канале, обычно центральный абонент может обслуживать не более 10 периферийных абонентов из-за большого падения скорости.

В большинстве случаев, например для объединения нескольких районов в городе, используют комбинированные топологии.

Режим повторителя

Может возникнуть ситуация, когда оказывается невозможно (неудобно) соединить точку доступа с проводной инфраструктурой или какое-либо препятствие затрудняет осуществление связи точки доступа с местом расположения беспроводных станций клиентов напрямую. В такой ситуации можно использовать точку в режиме повторителя (Repeater) (рис. 4.21).



Режим повторителя

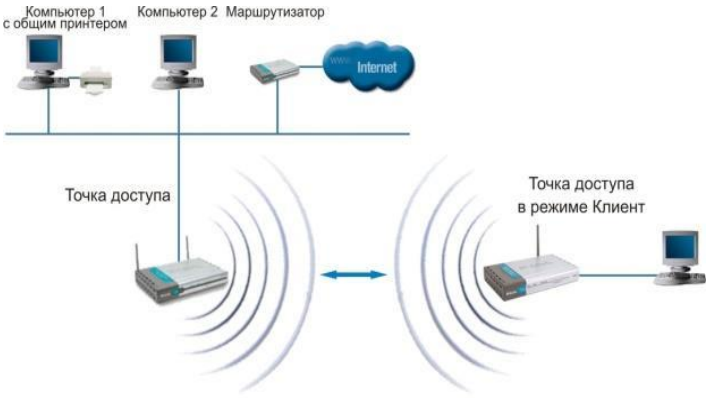
Аналогично проводному повторителю, беспроводной повторитель просто ретранслирует все пакеты, поступившие на его беспроводной интерфейс. Эта ретрансляция осуществляется через тот же канал, через который они были получены.

При применении точки доступа в режиме повторителя следует помнить, что наложение широковещательных доменов может привести к сокращению пропускной способности канала вдвое, потому что начальная точка доступа также "слышит" ретранслированный сигнал.

Режим повторителя не включен в стандарт 802.11, поэтому для его реализации рекомендуется использовать однотипное оборудование (вплоть до версии прошивки) и от одного производителя. С появлением WDS данный режим потерял свою актуальность, потому что WDS заменяет его. Однако его можно встретить в старых версиях прошивок и в устаревшем оборудовании.

Режим клиента

При переходе от проводной архитектуры к беспроводной иногда можно обнаружить, что имеющиеся сетевые устройства поддерживают проводную сеть Ethernet, но не имеют интерфейсных разъемов для беспроводных сетевых адаптеров. Для подключения таких устройств к беспроводной сети можно использовать точку доступа "клиент" (рис. 4.22).



Режим клиента

При помощи точки доступа, функционирующей в режиме клиента, к беспроводной сети подключается только одно устройство. Этот режим не включен в стандарт 802.11 и поддерживается не всеми производителями.

Роуминг - это возможность радиоустройства перемещаться за пределы действия базовой станции и, находясь в зоне действия "гостевой" станции, иметь доступ к "домашней" сети

При организации роуминга все точки доступа, обеспечивающие роуминг, конфигурируются на использование одинакового идентификатора зоны обслуживания (SSID). Все точки доступа относятся к одному широковещательному домену, или одному домену роуминга.

Механизм определения момента времени, когда необходимо начать процесс роуминга, не определен в стандарте 802.11, и, таким образом, оставлен на усмотрение поставщиков оборудования. Наиболее простой широко распространенный алгоритм переключения заключается в том, что адаптер взаимодействует с одной точкой вплоть до того момента, когда уровень сигнала не упадет ниже допустимого предела. После этого осуществляется поиск точки доступа с одинаковым SSID и максимальным уровнем сигнала, и переподключение к ней.

Роуминг включает значительно больше процессов, чем необходимо для поиска точки доступа, с которой можно связаться. Опишем некоторые из задач, которые должны решаться в ходе роуминга на канальном уровне:

- Предыдущая точка доступа должна определить, что клиент уходит из ее области действия.
- Предыдущая точка доступа должна буферизовать данные, предназначенные для клиента, осуществляющего роуминг.
- Новая точка доступа должна показать предыдущей, что клиент успешно переместился в ее зону.

- Предыдущая точка доступа должна послать буферизованные данные новой точке доступа.
- Предыдущая точка доступа должна определить, что клиент покинул ее зону действия.
- Точка доступа должна обновить таблицы MAC-адресов на коммутаторах инфраструктуры, чтобы избежать потери данных перемещающегося клиента.

Wi-Fi Direct *(ранее известный как **Wi-Fi Peer-to-Peer**)* — стандарт (набор программных протоколов), позволяющих двум и более Wi-Fi-устройствам общаться друг с другом без маршрутизаторов и хот-спотов.

О стандарте

Wi-Fi Direct позволяет организовывать беспроводные сети между компьютерами или, например, между компьютерами и периферийными устройствами, такими как принтер.

Wi-Fi Direct разрабатывается и поддерживается группой WECA — альянсом крупнейших производителей Wi-Fi-оборудования.

Самым близким аналогом Wi-Fi Direct являются старые специальные сети, ранний вариант Wi-Fi, который связывал 2 или более устройств без роутера.

Скорость передачи данных в стандарте будет соответствовать обычному соединению Wi-Fi. Стандарт позволит объединить как два устройства, так и несколько устройств между собой. Поддержка стандарта может быть встроена в самые различные устройства, такие, например как: коммуникаторы, телефоны, принтеры, цифровые фото/видеокамеры, клавиатуры и другие.

Лекция 7. Особенности использования сетей WiFi

1. Как жить хорошо самому и не мешать соседям.

Не только сигнал точки доступа должен достичь клиента, но и сигнал клиента должен достичь точки. Мощность передатчика ТД обычно до 100 мВт (20 dBm). А теперь загляните в datasheet к своему ноутбуку/телефону/планшету и найдите там мощность его Wi-Fi передатчика. Часто её вообще не указывают (можно поискать по FCC ID). Тем не менее, можно уверенно заявлять, что мощность типичных мобильных клиентов находится в диапазоне 30-50 мВт. Таким образом, если ТД вещает на 100мВт, а клиент – только на 50мВт, в зоне покрытия найдутся места, где клиент будет слышать точку хорошо, а ТД клиента — плохо (или вообще слышать не будет) – асимметрия. *Это справедливо даже с учетом того, что у точки обычно лучше чувствительность приема — смотрите под спойлером. Опять же,*

речь идет не о дальности, а о симметрии. Сигнал есть – а связи нет. Или downlink быстрый, а uplink медленный. Это актуально, если вы используете Wi-Fi для онлайн-игр или скайпа, для обычного интернет-доступа это не так и важно (только, если вы не на краю покрытия). И будем жаловаться на убогого провайдера, глючную точку, кривые драйвера, но не на неграмотное планирование сети.

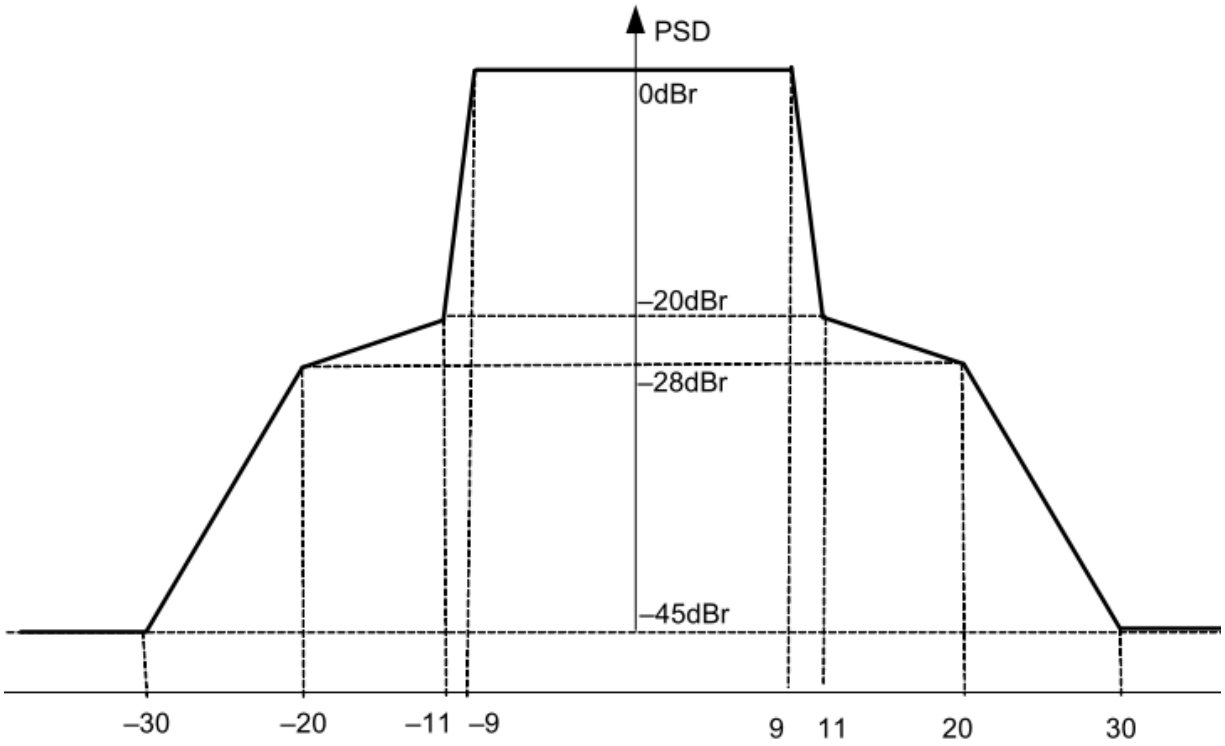
Вывод: может оказаться, что для получения более стабильной связи мощность точки придется снизить. Что, согласитесь, не совсем очевидно. Также далеко не самым известным фактом, добавляющим к асимметрии, является то, что у большинства клиентских устройств мощность передатчика снижена на «крайних» каналах (1 и 11/13 для 2.4 ГГц). Вот пример для iPhone из документации FCC (мощность на порту антенны).

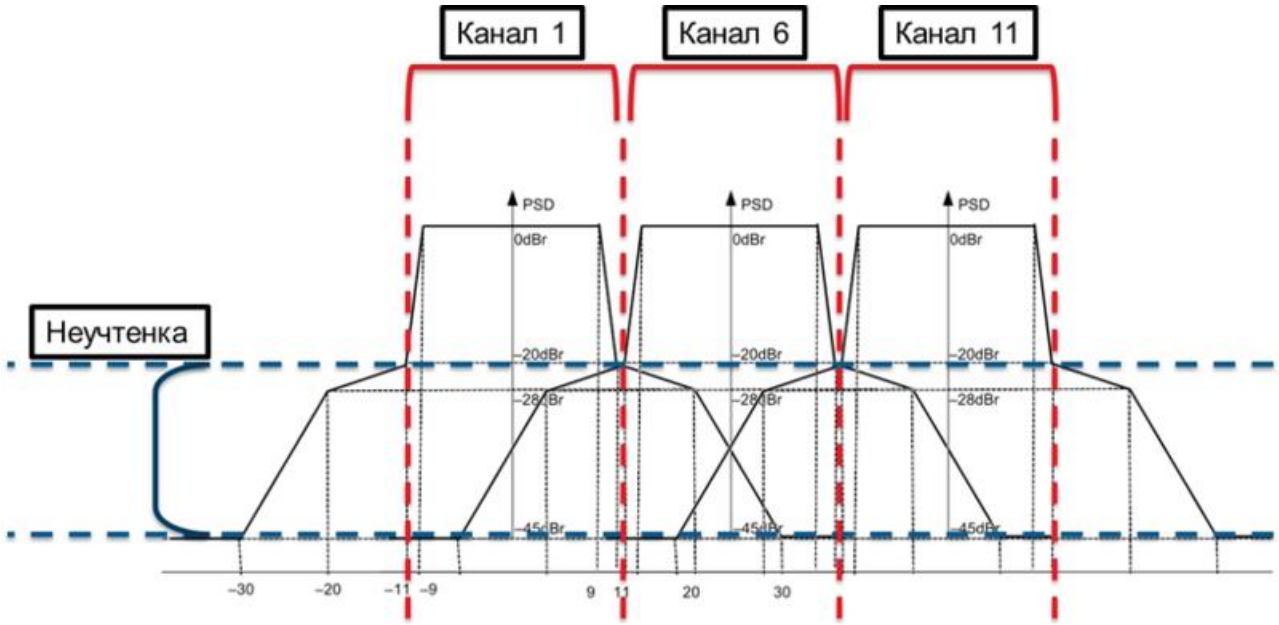
Channel	Frequency (MHz)	Power (dBm)
Low	2412	13.50
Middle	2437	17.00
High	2462	13.50

Как видите, на крайних каналах мощность передатчика в ~2.3 раза ниже, чем на средних. Причина в том, что Wi-Fi – связь широкополосная, удержать сигнал чётко в пределах рамки канала не удастся. Вот и приходится снижать мощность в «пограничных» случаях, чтобы не задевать соседние с ISM диапазоны. **Вывод: если ваш планшет плохо работает в туалете – попробуйте переехать на канал 6.**

2. Каналы WiFi

Всем известны «непересекающиеся» каналы 1/6/11. Так вот, они пересекаются! Потому, что Wi-Fi, как было упомянуто раньше, технология широкополосная и полностью сдержать сигнал в рамках канала невозможно. Приведенные ниже иллюстрации демонстрируют эффект для 802.11n OFDM (HT). На первой иллюстрации изображена спектральная маска 802.11n OFDM (HT) для 20МГц канала в 2.4ГГц (взята прямо из стандарта). По вертикали — мощность, по горизонтали — частота (смещение от центральной частоты канала). На второй иллюстрации я наложил спектральные маски каналов 1,6,11 с учетом соседства. Из этих иллюстраций мы сделаем два важных вывода.





Все считают, что ширина канала — 22МГц (так и есть). Но, как показывает иллюстрация, сигнал на этом не заканчивается, и даже непересекающиеся каналы таки перекрываются: 1/6 и 6/11 — на ~-20dBr, 1/11 — на ~-36dBr, 1/13 — на -45dBr. Попытка поставить две точки доступа, настроенные на соседние «неперекрывающиеся» каналы, близко друг от друга приведет к тому, что каждая из них будет создавать соседке помеху в 20dBm – 20dB – 50dB [которые добавим на потери распространения сигнала на малое расстояние и небольшую стенку] =-50dBm! Такой уровень шума способен целиком забить любой полезный Wi-Fi сигнал из соседней комнаты, или блокировать ваши коммуникации целиком!

Почему

В 802.11 используется метод доступа к среде CSMA/CA (обычно, по методу EDCA/HCF, кому интересно, читайте про 802.11e). Для определения занятости канала используется механизм CCA (Clear Channell Assesment). Вот выдержка из

стандарта: *The receiver shall hold the CCA signal busy for any signal 20 dB or more above the minimum modulation and coding rate sensitivity (–82 + 20 = –62 dBm) in the 20 MHz channel.* Соответственно станция (точка или клиент) считает эфир занятым, если слышит сигнал -62dBm и выше, независимо то того, велась ли передача на том же канале, на соседнем, или это вообще микроволновка работает. В случае клиента все еще не так плохо, но если у вас помеха в >=-62dBm в районе точки — будет страдать вся ячейка. По той же причине все серьезные вендоры просто не выпускают dual-radio ТД, в которых оба модуля могут работать в 2.4 одновременно: легче запретить, чем каждый раз объяснять.
Вывод: если вы поставите точку рядом со стеной, а ваш сосед – с другой стороны стены, его точка на соседнем «неперекрывающемся» канале все равно может доставлять вам серьезные проблемы.

Попробуйте посчитать значения помехи для каналов 1/11 и 1/13 и сделать выводы самостоятельно. Аналогично, некоторые стараются «уплотнить» покрытие, устанавливая две точки настроенные на разные каналы друг на друга стопкой — думаю, уже не надо объяснять, что будет (исключением тут будет грамотное экранирование и грамотное разнесение антенн — все возможно, если знать как).
Второй интересный аспект – это попытки чуть более продвинутых пользователей «убежать» между стандартными каналами 1/6/11. Опять же, логика проста: «Я между каналами словлю меньше помех». По факту, помех, обычно, ловится не меньше, а больше. Раньше вы страдали по полной только от одного соседа (на том же канале, что и вы). Но это были помехи не первого уровня OSI (интерференция), а второго – коллизии — т.к. ваша точка делила с соседом коллизионный домен и цивилизованно соседствовала на MAC-уровне. Теперь вы ловите интерференцию (Layer1) от двух соседей с обеих сторон.
В итоге, delay и jitter, может, и попытались немного уменьшиться (т.к. коллизий теперь как бы нет), но зато уменьшилось и соотношение сигнал/шум. А с ним уменьшились и скорости (т.к. каждая скорость требует некоторого минимального SNR) и процент годных фреймов (т.к. уменьшился запас по SNR, увеличилась чувствительность к случайным всплескам интерференции). Как следствие, обычно, возростает retransmit rate, delay, jitter, уменьшается пропускная способность. Кроме того, при значительном перекрытии каналов таки возможно корректно принять фрейм с соседнего канала (если соотношение сигнал/шум позволяет) и таки получить коллизию. А при помехе выше -62dBm вышеупомянутый механизм CCA просто не даст воспользоваться каналом. Это только усугубляет ситуацию и негативно влияет на пропускную способность.
Вывод: не старайтесь использовать нестандартные каналы, не просчитав последствий, и отговаривайте от этого соседей. В общем, то же, что и с мощностью: отговаривайте соседей врубать точки на полную мощность на нестандартных каналах – будет меньше интерференции и коллизий у всех. Как просчитать последствия станет понятно из [3].

По примерно тем же причинам не стоит ставить точку доступа у окна, если только вы не планируете пользоваться/раздавать Wi-Fi во дворе. Толку от того, что ваша точка будет светить вдаль, вам лично никакого – зато будете собирать коллизии и шум от всех соседей в прямой видимости. И сами к захламленности эфира добавите. Особенно в многоквартирных домах, построенных зигзагами, где окна соседей смотрят друг на друга с расстояния в 20-30м. Соседям с точками на подоконниках принесите свинцовой краски на окна.

Также, для 802.11n актуален вопрос 40MHz каналов. Моя рекоммендация — включать 40MHz в режим «авто» в 5GHz, и не включать («20MHz only») в 2.4GHz (исключение — полное отсутствие соседей). Причина в том, что в присутствии 20MHz-соседей вы с большой долей вероятности получите помеху на одной из половин 40MHz-канала + включится режим совместимости 40/20MHz. Конечно, можно жестко зафиксировать 40MHz (если все ваши клиенты его поддерживают), но помеха все равно останется. Как по мне, лучше стабильные 75Mbps на поток, чем нестабильные 150. Опять же, возможны исключения.

3. Раз уж речь зашла о скоростях…

Уже несколько раз мы упоминали скорости (rate/MCS — не throughput) в связке с SNR. Ниже приведена таблица необходимых SNR для рейтов/MCS, составленная мной по материалам стандарта. Собственно, именно поэтому для более высоких скоростей чувствительность приемника меньше, как мы заметили в [1.1].

	Rate (Mbps)	SNR (dB)
802.11b	1	4
DSSS	2	6
	5.5	8
	11	10
802.11a/g	6	5
OFDM	9	8
	12	10
	18	13
	24	16
	36	19
	48	22
	54	25

802.11n MCS	SNR (dB) 20Mhz/40Mhz
0/8/…	5
1/9/…	10
2/10/…	13
3/11/…	16
4/12/…	19
5/13/…	22
6/14/…	25
7/15/…	28

В сетях 802.11n/MIMO благодаря MRC и другим многоантенным ухищрениям нужный SNR можно получить и при более низком входном сигнале. Обычно, это отражено в значениях чувствительности в datasheet'ax.
Отсюда, кстати, можно сделать еще один вывод: **эффективный размер (и форма) зоны покрытия зависит от выбранной скорости (rate/MCS).** Это важно учитывать в своих ожиданиях и при планировании сети.

Этот пункт может оказаться неосуществимым для владельцев точек доступа с совсем простыми прошивками, которые не позволяют выставлять Basic и Supported Rates. Как уже было сказано выше, скорость (rate) зависит от соотношения сигнал/шум. Если, скажем, 54Mbps требует SNR в 25dB, а 2Mbps требует 6dB, то понятно, что фреймы, отправленные на скорости 2Mbps «пролетят» дальше, т.е.

их можно декодировать с большего расстояния, чем более скоростные фреймы. Тут мы и приходим к Basic Rates: все служебные фреймы, а также броадкасты (если точка не поддерживает BCast/MCast acceleration и его разновидности), отправляются на самой нижней Basic Rate. А это значит, что вашу сеть будет видно за многие кварталы. Вот пример (спасибо Motorola AirDefense).

Опять же, это добавляет к рассмотренной в картине коллизий: как для ситуации с соседями на том же канале, так и для ситуации с соседями на близких перекрывающихся каналах. Кроме того, фреймы ACK (которые отправляются в ответ на любой unicast пакет) тоже ходят на минимальной Basic Rate (если точка не поддерживает их акселерацию)

Вывод: отключайте низкие скорости – и у вас, и у соседей сеть станет работать быстрее. У вас – за счет того, что весь служебный трафик резко начнет ходить быстрее, у соседей – за счет того, что вы теперь для них не создаете коллизий (правда, вы все еще создаете для них интерференцию — сигнал никуда не делся — но обычно достаточно низкую). Если убедите соседей сделать то же самое – у вас сеть будет работать еще быстрее.

Понятно, что при отключении низких скоростей подключиться к тоже можно будет только в зоне более сильного сигнала (требования к SNR стали выше), что ведет к уменьшению эффективного покрытия. Равно как и в случае с понижением мощности. Но тут уж вам решать, что вам нужно: максимальное покрытие или быстрая и стабильная связь. Используя табличку и datasheet'ы производителя точки и клиентов почти всегда можно достичь приемлемого баланса.

Еще одним интересным вопросом являются режимы совместимости (т.н. “Protection

Modes”). В настоящее время есть режим совместимости b-g (ERP Protection) и a/g-n (HT Protection). В любом случае скорость падает. На то, насколько она падает, влияет куча факторов (тут еще на две статьи материала хватит), я обычно просто говорю, что скорость падает примерно на треть. При этом, если у вас точка 802.11n и клиент 802.11n, но у соседа за стеной точка g, и его трафик долетает до вас – ваша точка точно так же свалится в режим совместимости, ибо того требует стандарт. Особенно приятно, если ваш сосед – самоделкин и ваяет что-то на основе передатчика 802.11b. :) Что делать? Так же, как и с уходом на нестандартные каналы – оценить, что для вас существеннее: коллизии (L2) или интерференция (L1). **Если уровень сигнала от соседа относительно низок, переключайте точки в режим чистого 802.11n (Greenfield)**: возможно, понизится максимальная пропускная способность (снизится SNR), но трафик будет ходить равномернее из-за избавления от избыточных коллизий, пачек защитных фреймов и переключения модуляций. В противном случае – лучше терпеть и поговорить с соседом на предмет мощности/перемещения ТД. Ну, или отражатель поставить… Да, и не ставьте точку на окно! :)

Другой вариант – переезжать в 5 ГГц, там воздух чище: каналов больше, шума меньше, сигнал ослабляется быстрее, да и банально точки стоят дороже, а значит – их меньше. Многие покупают dual radio точку, настраивают 802.11n Greenfield в 5 ГГц и 802.11g/n в 2.4 ГГц для гостей и всяких гаджетов, которым скорость все равно не нужна. Да и безопаснее так: у большинства script kiddies нет денег на дорогие игрушки с поддержкой 5 ГГц.
Для 5 ГГц следует помнить, что надежно работают только 4 канала: 36/40/44/48 (для Европы, для США есть еще 5). На остальных включен режим сосуществования с радарами (DFS). В итоге, связь может периодически пропадать.

4. Раз уж речь зашла о безопасности…

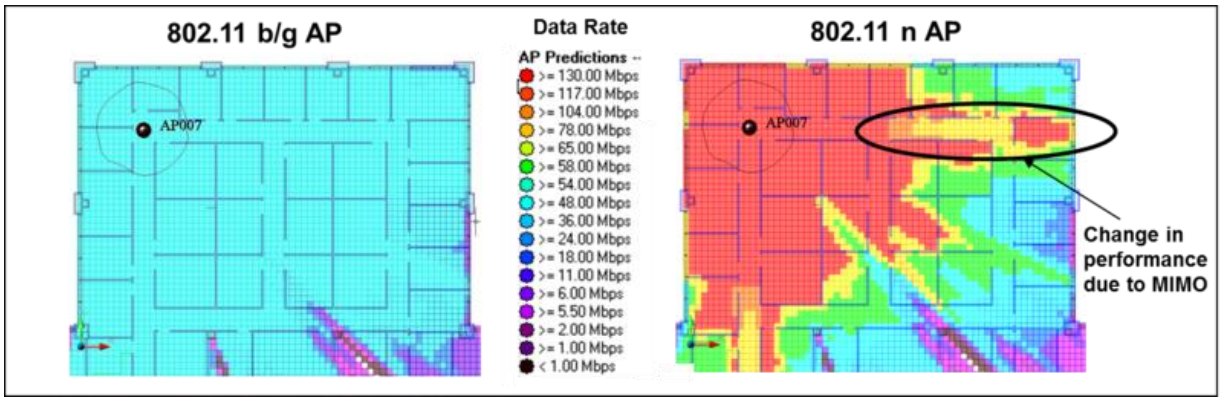
Упомянем некоторые интересные аспекты и здесь.
Какой должна быть длина PSK? Вот выдержка из текста стандарта 802.11-2012, секция M4.1:
Keys derived from the pass phrase provide relatively low levels of security, especially with keys generated form short passwords, since they are subject to dictionary attack. Use of the key hash is recommended only where it is impractical to make use of a stronger form of user authentication. A key generated from a passphrase of less than about 20 characters is unlikely to deter attacks.

Почему моя точка 802.11n не «разгоняется» выше скоростей a/g? И какое отношение это имеет к безопасности? Стандарт 802.11n поддерживает только два режима шифрования: CCMP и None. Сертификация Wi-Fi 802.11n Compatible требует, чтобы при включении TKIP на радио точка переставала поддерживать все новые скоростные режимы 802.11n, оставляя лишь скорости 802.11a/b/g. В некоторых случаях можно видеть ассоциации на более высоких рейтах, но пропускная способность все равно будет низкой. **Вывод: забываем про TKIP**.

5. Всякая всячина.

Немного о MIMO. По сей день я сталкиваюсь с формулировками типа 2x2 MIMO или 3x3 MIMO. К сожалению, для 802.11n эта формулировка малополезна, т.к. важно знать еще количество пространственных потоков (Spatial Streams). Точка 2x2 MIMO может поддерживать только один SS, и не поднимется выше 150Mbps. Точка с 3x3 MIMO может поддерживать 2SS, ограничиваясь лишь 300Mbps. Полная формула MIMO выглядит так: TX x RX: SS. Понятно, что количество SS не может быть больше min (TX, RX). Таким образом, приведенные выше точки будут записаны как 2x2:1 и 3x3:2. Многие беспроводные клиенты реализуют 1x2:1 MIMO (смартфоны, планшеты, дешевые ноутбуки) или 2x3:2 MIMO. **Так что бесполезно ожидать скорости 450Mbps от точки доступа 3x3:3 при работе с клиентом 1x2:1.** Тем не менее, **покупать точку типа 2x3:2 все равно стоит**, т.к. большее количество принимающих антенн добавляет точке чувствительности (MRC Gain). Чем больше разница между количеством принимающих антенн точки и количеством передающих антенн клиента — тем больше выигрыш (если на пальцах). Однако, в игру вступает multipath.

Как известно, multipath для сетей 802.11a/b/g – зло. Точка доступа, поставленная антенной в угол, может работать не самым лучшим образом, а выдвинутая из этого угла на 20-30см может показать значительно лучший результат. Аналогично для клиентов, помещений со сложной планировкой, кучей металлических предметов и т.д.
Для сетей MIMO с MRC и в особенности для работы нескольких SS (и следовательно, для получения высоких скоростей) multipath – необходимое условие. Ибо, если его не будет – создать несколько пространственных потоков не получится. Предсказывать что-либо без специальных инструментов планирования здесь сложно, да и с ними непросто. Вот пример рассчетов из Motorola LANPlanner, но однозначный ответ тут может дать только радиоразведка и тестирование.



Создать благоприятную multipath-обстановку для работы трех SS сложнее, чем для работы двух SS. Поэтому новомодные точки 3x3:3 работают с максимальной производительностью обычно лишь в небольшом радиусе, да и то не всегда.

Ну, и несколько интересных фактов для коллекции:

- Человеческое тело ослабляет сигнал на 3-5dB (2.4/5ГГц). Просто развернувшись лицом к точке можно получить более высокую скорость.
- Некоторые дипольные антенны имеют асмммметричную диаграмму направленности в H-плоскости («вид сбоку») и лучше работают перевернутыми

- В фрейме 802.11 может использоваться одновременно до четырех MAC-адресов, а в 802.11s (новый стандарт на mesh) — до шести!

Итого

Технология 802.11 (да и радиосетей в целом) обладает множеством неочевидных особенностей. Лично у меня вызывает громадное уважение и восхищение тот факт, что люди отточили насколько сложную технологию до уровня «воткни-работай». Мы рассмотрели (в разном объеме) разные аспекты физического и канального уровня сетей 802.11:

- Асиметрию мощностей
- Ограничения на мощность передачи в граничных каналах
- Пересечение «непересекающихся» каналов и последствия
- Работу на «нестандартных» каналах (отличных от 1/6/11/13)
- Работу механизма Clear Channel Assesment и блокировку канала
- Зависимость скорости (rate/MCS) от SNR и, как следствие, зависимость чувствительности приемника и зоны покрытия от требуемой скорости
- Особенности пересылки служебного трафика
- Последствия включения поддержки низких скоростей
- Последствия включения поддержки режимов совместимости
- Выбор каналов в 5ГГц
- Некоторые забавные аспекты безопасности, MIMO и проч.

Не все было рассмотрено в полном объеме и исчерпывающем виде, равно как за бортом остались неочевидные аспекты сосуществования клиентов, балансировки нагрузки, WMM, питания и роуминга, экзотика типа Single-Channel Architecture и индивидуальных BSS — но это уже тема для сетей совсем другого масштаба. Если следовать хотя бы вышеприведенным соображениям, в обычном жилом доме можно получить вполне приличный коммунизм microcell, как в высокопроизводительных корпоративных WLAN.

Лекция 8. Защита в Wi-Fi сетях

В Hot-spot сетях присутствует точка доступа (англ. Access point), посредством которой происходит не только взаимодействие внутри сети, но и доступ к внешним сетям. Hot-spot представляет наибольший интерес с точки зрения защиты информации, т.к., взломав точку доступа, злоумышленник может получить информацию не только со станций, размещенных в данной беспроводной сети.

Методы ограничения доступа

Фильтрация MAC-адресов:

Данный метод не входит в стандарт IEEE 802.11. Фильтрацию можно осуществлять тремя способами:

- Точка доступа позволяет получить доступ станциям с любым MAC-адресом;
- Точка доступа позволяет получить доступ только станциям, чьи MAC-адреса находятся в доверительном списке;
- Точка доступа запрещает доступ станциям, чьи MAC-адреса находятся в “чёрном списке”;

Наиболее надежным с точки зрения безопасности является второй вариант, хотя он не рассчитан на подмену MAC-адреса, что легко осуществить злоумышленнику.

Режим скрытого идентификатора SSID (англ. Service Set IDentifier):

Для своего обнаружения точка доступа периодически рассылает кадры-маячки (англ. beacon frames). Каждый такой кадр содержит служебную информацию для подключения и, в частности, присутствует SSID (идентификатор беспроводной сети). В случае скрытого SSID это поле пустое, т.е. невозможно обнаружение вашей беспроводной сети и нельзя к ней подключиться, не зная значение SSID . Но все станции в сети, подключенные к точке доступа, знают SSID и при подключении, когда рассылают Probe Request запросы, указывают идентификаторы сетей, имеющиеся в их профилях подключений. Прослушивая рабочий трафик, с легкостью можно получить значение SSID, необходимое для подключения к желаемой точке доступа.

Методы аутентификации

Аутентификация - выдача определённых прав доступа абоненту на основе имеющегося у него идентификатора.

IEEE 802.11 предусматривает два метода аутентификации:

1. Открытая аутентификация (англ. Open Authentication):

Рабочая станция делает запрос аутентификации, в котором присутствует только MAC-адрес клиента. Точка доступа отвечает либо отказом, либо подтверждением аутентификации. Решение принимается на основе MAC-фильтрации, т.е. по сути это защита беспроводной Wi-Fi сети на основе ограничения доступа, что не безопасно.

2. Аутентификация с общим ключом (англ. Shared Key Authentication):

Необходимо настроить статический ключ шифрования алгоритма WEP (англ. Wired Equivalent Privacy). Клиент делает запрос у точки доступа на аутентификацию, на что получает подтверждение, которое содержит 128 байт случайной информации. Станция шифрует полученные данные алгоритмом WEP (проводится побитовое сложение по модулю 2 данных сообщения с последовательностью ключа) и отправляет зашифрованный текст вместе с запросом на ассоциацию. Точка доступа расшифровывает текст и сравнивает с исходными данными. В случае совпадения отсылается подтверждение ассоциации, и клиент считается подключенным к сети.

Схема аутентификации с общим ключом уязвима к атакам «Man in the middle». Алгоритм шифрования WEP – это простой XOR ключевой последовательности с полезной информацией, следовательно, прослушав трафик между станцией и точкой доступа, можно восстановить часть ключа.

IEEE начал разработки нового стандарта IEEE 802.11i, но из-за трудностей утверждения, организация WECA (англ. Wi-Fi Alliance) совместно с IEEE анонсировали стандарт WPA (англ. Wi-Fi Protected Access). В WPA используется TKIP (англ. Temporal Key Integrity Protocol, протокол проверки целостности ключа), который использует усовершенствованный способ управления ключами и покадровое изменение ключа.

WPA также использует два способа аутентификации:

- Аутентификация с помощью предустановленного ключа WPA-PSK (англ. Pre-Shared Key) (Enterprise Autentification);
- Аутентификация с помощью RADIUS-сервера (англ. Remote Access Dial-in User Service)

Методы шифрования

WEP-шифрование (англ. Wired Equivalent Privacy):

Wired Equivalent Privacy (WEP) — алгоритм для обеспечения безопасности сетей Wi-Fi. Используется для обеспечения конфиденциальности и защиты передаваемых данных авторизированных пользователей беспроводной сети от прослушивания. Существует две разновидности WEP: WEP-40 и WEP-104, различающиеся только длиной ключа. В настоящее время данная технология является устаревшей, так как ее взлом может быть осуществлен всего за несколько минут. Тем не менее, она продолжает широко использоваться. Для безопасности в сетях Wi-Fi рекомендуется использовать WPA. WEP часто неправильно называют Wireless Encryption Protocol.

В 1997 году Институт Инженеров Электротехники и Радиоэлектроники (IEEE) одобрил механизм WEP. В октябре 2000-го года вышла статья Джесси Уолкера «Unsafe at any key size; An analysis of the WEP encapsulation», описывающая проблемы алгоритма WEP и атаки, которые могут быть организованы с использованием его уязвимостей. В алгоритме есть множество слабых мест:

- механизмы обмена ключами и проверки целостности данных,
- малая разрядность ключа и вектора инициализации (англ. Initialization vector),
- способ аутентификации,
- алгоритм шифрования.

В 2001 году появилась спецификация WEP-104, которая, тем не менее, не решила проблемы, так как длина вектора инициализации и способ проверки целостности данных остались прежними. В 2004 году IEEE одобрил новые механизмы WPA и WPA2. С тех пор WEP считается устаревшим. В 2008 году вышел стандарт DSS (англ. Data Security Standard) комитета SSC (англ. Security Standards Council) организации PCI (англ. Payment Card Industry) в котором рекомендуется прекратить использовать WEP для шифрования после 30 июня 2010 года.

В основе WEP лежит поточный шифр RC4, выбранный из-за своей высокой скорости работы и возможности использования переменной длины ключа. Для подсчета контрольных сумм используется CRC32.

Кадр WEP включает в себя следующие поля:

Незашифрованная часть

Вектор инициализации (англ. Initialization Vector) (24 бита)

Пустое место (англ. Padding) (6 бит)

Идентификатор ключа (англ. Key ID) (2 бита)

Зашифрованная часть

Данные

Контрольная сумма (32 бита)

Ключи имеют длину 40 и 104 бита для WEP-40 и WEP-104 соответственно. Используются два типа ключей: ключи по умолчанию и назначенные ключи. Назначенный ключ отвечает определенной паре отправитель-получатель. Может иметь любое, заранее оговоренное сторонами значение. Если же стороны предпочтут не использовать назначенный ключ, им выдается один из четырех ключей по умолчанию из специальной таблицы. Для каждого кадра данных создается сид (англ. Seed), представляющий собой ключ с присоединенным к нему вектором инициализации.

Инкапсуляция WEP данных проходит следующим образом:

1. Контрольная сумма от поля «данные» вычисляется по алгоритму CRC32 и добавляется в конец кадра.
2. Данные с контрольной суммой шифруются алгоритмом RC4, использующим в качестве ключа криптоалгоритма.
3. Проводится операция XOR над исходным текстом и шифротекстом.
4. В начало кадра добавляется вектор инициализации и идентификатор ключа.

Декапсуляция данных проходит следующим образом:

1. К используемому ключу добавляется вектор инициализации.
2. Происходит расшифрование с ключом, равным сиду.
3. Проводится операция XOR над полученным текстом и шифротекстом.
4. Проверяется контрольная сумма.

Проблемы

Все атаки на WEP основаны на недостатках шифра RC4, таких, как возможность коллизий векторов инициализации и изменения кадров. Для всех типов атак

требуется проводить перехват и анализ кадров беспроводной сети. В зависимости от типа атаки, количество кадров, требуемое для взлома, различно. С помощью программ, таких как Aircrack-ng, взлом беспроводной сети с WEP шифрованием осуществляется очень быстро и не требует специальных навыков.

Атака Фларера-Мантина-Шамира (англ.)

Была предложена в 2001 году Скоттом Фларером, Ициком Мантином и Ади Шамиром. Требует наличия в кадрах слабых векторов инициализации. В среднем для взлома необходимо перехватить около полумиллиона кадров. При анализе используются только слабые векторы. При их отсутствии (например, после коррекции алгоритма шифрования) данная атака неэффективна.

Атака KoreK

В 2004 году была предложена хакером, называющим себя KoreK.[2] Ее особенность в том, что для атаки не требуются слабые вектора инициализации. Для взлома необходимо перехватить несколько сотен тысяч кадров. При анализе используются только векторы инициализации.

Атака Тевса-Вайнмана-Пышкина

Была предложена в 2007 году Эриком Тевсом (Erik Tews), Ральфом-Филипом Вайнманом (Ralf-Philipp Weinmann) и Андреем Пышкиным. Использует возможность инъекции ARP запросов в беспроводную сеть. На данный момент это наиболее эффективная атака, для взлома требуется всего несколько десятков тысяч кадров. При анализе используются кадры целиком.

Решения

Использование туннелирования через беспроводную сеть (например, с помощью IPSec) решает проблему безопасности. Тем не менее, существуют решения, делающие сеть безопасной саму по себе.

802.11i

В 2004 году IEEE выпустил поправку к стандарту 802.11, включающую в себя новые рекомендуемые к использованию алгоритмы обеспечения безопасности WPA и WPA2. WEP был объявлен устаревшим.

Решения от производителей

Также существуют решения, реализуемые конкретными производителями в своих устройствах. Эти решения существенно менее безопасны, чем WPA и WPA2, так как подвержены (хоть и в меньшей степени) тем же уязвимостям, что и WEP.

WEP 2

Увеличивает векторы инициализации и ключи до 128 бит.

WEP Plus

Избегает слабых векторов инициализации. Эффективен только в том случае, если алгоритм используется на обеих сторонах соединения.

Dynamic WEP

Динамически меняет ключи при передаче.

TKIP-шифрование (англ. Temporal Key Integrity Protocol):

Используется тот же симметричный потоковый шифр RC4, но является более криптостойким. Вектор инициализации составляет 48 бит. Учтены основные атаки на WEP. Используется протокол Message Integrity Check для проверки целостности сообщений, который блокирует станцию на 60 секунд, если были посланы в течение 60 секунд два сообщения не прошедших проверку целостности. С учетом всех доработок и усовершенствований TKIP все равно не считается криптостойким.

CKIP-шифрование (англ. Cisco Key Integrity Protocol):

Имеет сходства с протоколом TKIP. Создан компанией Cisco. Используется протокол CMIC (англ. Cisco Message Integrity Check) для проверки целостности сообщений.

WPA

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

В WPA обеспечена поддержка стандартов 802.1X, а также протокола EAP (Extensible Authentication Protocol, расширяемый протокол аутентификации). Стоит заметить, что в WPA2 поддерживается шифрование в соответствии со стандартом AES (Advanced Encryption Standard, усовершенствованный стандарт шифрования), который имеет ряд преимуществ над используемым в WEP RC4, например гораздо более стойкий криптоалгоритм.

Большим плюсом при внедрении EWPA является возможность работы технологии на существующем аппаратном обеспечении Wi-Fi.

Некоторые отличительные особенности WPA:

- усовершенствованная схема шифрования RC4
- обязательная аутентификация с использованием EAP.
- система централизованного управления безопасностью, возможность использования в действующих корпоративных политиках безопасности.

Wi-Fi Alliance даёт следующую формулу для определения сути WPA:

WPA = 802.1X + EAP + TKIP + MIC

Видно, что WPA, по сути, является суммой нескольких технологий.

Как упомянуто выше, в стандарте WPA используется Расширяемый протокол аутентификации (EAP) как основа для механизма аутентификации пользователей. Непременным условием аутентификации является предъявление пользователем свидетельства (иначе называют мандатом), подтверждающего его право на доступ

в сеть. Для этого права пользователь проходит проверку по специальной базе зарегистрированных пользователей. Без аутентификации работа в сети для пользователя будет запрещена. База зарегистрированных пользователей и система проверки в больших сетях как правило расположены на специальном сервере (чаще всего RADIUS).

Следует отметить, что WPA имеет упрощённый режим. Он получил название Pre-Shared Key (WPA-PSK). При применении режима PSK необходимо ввести один пароль для каждого отдельного узла беспроводной сети (беспроводные маршрутизаторы, точки доступа, мосты, клиентские адаптеры). Если пароли совпадают с записями в базе, пользователь получит разрешение на доступ в сеть.

Даже не принимая во внимания тот факт что WEP, предшественник WPA, не обладает какими-либо механизмами аутентификации пользователей как таковой, его ненадёжность состоит, прежде всего, в криптографической слабости алгоритма шифрования. Ключевая проблема WEP заключается в использовании слишком похожих ключей для различных пакетов данных.

TKIP, MIC и 802.1X (части уравнения WPA) внесли свою лепту в усиление шифрования данных сетей, использующих WPA.

TKIP отвечает за увеличение размера ключа с 40 до 128 бит, а также за замену одного статического ключа WEP ключами, которые автоматически генерируются и рассылаются сервером аутентификации. Кроме того, в TKIP используется специальная иерархия ключей и методология управления ключами, которая убирает излишнюю предсказуемость, которая использовалась для несанкционированного снятия защиты WEP ключей.

Сервер аутентификации, после получения сертификата от пользователя, использует 802.1X для генерации уникального базового ключа для сеанса связи. TKIP осуществляет передачу сгенерированного ключа пользователю и точке доступа, после чего выстраивает иерархию ключей плюс систему управления. Для этого используется двусторонний ключ для динамической генерации ключей шифрования данных, которые в свою очередь используются для шифрования каждого пакета данных. Подобная иерархия ключей TKIP заменяет один ключ WEP (статический) на 500 миллиардов возможных ключей, которые будут использованы для шифрования данного пакета данных.

Другим важным механизмом является проверка целостности сообщений (Message Integrity Check, MIC). Её используют для предотвращения перехвата пакетов

данных, содержание которых может быть изменено, а модифицированный пакет вновь передан по сети. MIC построена на основе мощной математической функции, которая применяется на стороне отправителя и получателя, после чего сравнивается результат. Если проверка показывает на несовпадение результатов вычислений, данные считаются ложными и пакет отбрасывается.

При этом механизмы шифрования, которые используются для WPA и WPA-PSK, являются идентичными. Единственное отличие WPA-PSK состоит в том, что аутентификация производится с использованием пароля, а не по сертификату пользователя.

WPA2 определяется стандартом IEEE 802.11i, принятым в июне 2004 года, и призван заменить WPA. В нём реализовано CCMP и шифрование AES, за счет чего WPA2 стал более защищённым, чем свой предшественник. С 13 марта 2006 года поддержка WPA2 является обязательным условием для всех сертифицированных Wi-Fi устройств.

6 ноября 2008 года на конференции PacSec был представлен способ, позволяющий взломать ключ TKIP, используемый в WPA, за 12-15 минут. Этот метод позволяет прочитать данные, передаваемые от точки доступа клиентской машине, а также передавать поддельную информацию на клиентскую машину. Данные, передаваемые от клиента к маршрутизатору, пока прочитать не удалось. Ещё одним условием успешной атаки было включение QoS на маршрутизаторе.

В 2009 году сотрудниками университета Хиросимы и университета Кобе, Тосихиру Оигаси и Масакату Мории был разработан и успешно реализован на практике новый метод атаки, который позволяет взломать любое WPA соединение без ограничений, причём, в лучшем случае, время взлома составляет 1 минуту.

Необходимо заметить, что соединения WPA, использующие более защищённый стандарт шифрования ключа AES, а также WPA2-соединения, не подвержены этим атакам.

23 июля 2010 года была опубликована информация об уязвимости Hole196 в протоколе WPA2. Используя эту уязвимость, авторизовавшийся в сети злонамеренный пользователь может расшифровывать данные других пользователей, используя свой закрытый ключ. Никакого взлома ключей или брут-форса не требуется.

Тем не менее, на данный момент основными методами взлома WPA2 PSK являются атака по словарю и брут-форс. Для этого в режиме мониторинга беспроводной карты сканируется эфир и записываются необходимые пакеты. Далее проводится деавторизация клиента для захвата начального обмена пакетами (handshake), либо нужно ждать пока клиент совершит подключение. После этого уже нет необходимости находиться недалеко от атакуемой точки доступа. Атака проводится оффлайн с помощью специальной программы и файла с хэндшейком.

16 октября 2017 года, было запланировано скоординированное раскрытие информации о критических проблемах WPA2, которые позволяют обойти защиту и прослушивать Wi-Fi-трафик, передаваемый между точкой доступа и компьютером.

Комплекс уязвимостей в WPA2 получил название KRACK (аббревиатура от **K**ey **R**einstallation Att**ack**s) и был обнаружен сводной группой исследователей, в которую вошли: Мэти Ванхоф (Mathy Vanhoef) и Фрэнк Писсенс (Frank Piessens) из Левенского католического университета, Малихех Ширванян (Maliheh Shirvanian) и Нитеш Саксена (Nitesh Saxena) из Алабамского университета в Бирмингеме, Ионг Ли (Yong Li) из компании Huawei Technologies, а также представитель Рурского университета Свен Шеге (Sven Schäge).

Исследователи пишут, что краеугольным камнем их атаки является четырехэлементный хендшейк WPA2. Данный хендшейк осуществляется тогда, когда клиент хочет подключиться к защищенной сети Wi-Fi. Он используется для подтверждения того, что обе стороны (клиент и точка доступа) обладают корректными учетными данными. В то же время хендшейк используется для согласования свежего ключа шифрования, который впоследствии будет применяться для защиты трафика. В настоящее время практически все защищенные Wi-Fi сети используют именно такой, четырехэлементный хендшейк. Что делает их все уязвимыми перед какой-либо вариацией атак KRACK.

«К примеру, атака работает против частных и корпоративных Wi-Fi сетей, против устаревшего WPA и свежего стандарта WPA2, и даже против сетей, которые используют исключительно AES. Все наши атаки, направленные на WPA2, используют новаторскую технику реинсталляции ключей (key reinstallation)», — пишут авторы KRACK.

По сути, KRACK позволяет злоумышленнику осуществить атаку типа man-in-the-middle и принудить участников сети выполнить реинсталляцию ключей шифрования, которые защищают трафик WPA2. К тому же если сеть настроена на использование WPA-TKIP или GCMP, злоумышленник сможет не только прослушивать трафик WPA2, но и осуществлять инжекты пакетов в данные жертвы.

Метод KRACK универсален и работает против любых устройств, подключенных к Wi-Fi сети. То есть в опасности абсолютно все пользователи Android, Linux, iOS, macOS, Windows, OpenBSD, а также многочисленные IoT-устройства. Единственной хорошей новостью на сегодня является тот факт, что атакующему придется находиться к зоне действия целевой Wi-Fi сети, то есть атаку не получится осуществить удаленно.

WPA3

Wi-Fi Alliance анонсировал долгожданное третье поколение протокола беспроводной безопасности — Wi-Fi Protected Access (WPA3).

WPA3 заменит существующий WPA2 — протокол сетевой безопасности, который существует не менее 15 лет и используется миллиардами беспроводных устройств каждый день.

Небезопасность WPA2 уже долгое время обсуждалась специалистами. Переломным моментом стал октябрь 2017 года, когда исследователь Мэти Ванхов (Mathy Vanhoef) обнаружил уязвимость в протоколе WPA2, ставящую под угрозу практически все существующие на данный момент сети Wi-Fi. С ее помощью злоумышленник может осуществить атаку реинсталяции ключей (Key Reinstallation Attack, KRACK) и получить доступ к конфиденциальным данным. Уязвимость вызвала серьезное беспокойство экспертов по безопасности, поскольку содержалась в самом протоколе WPA2.

Новый стандарт безопасности Wi-Fi, который будет доступен как для персональных, так и для корпоративных беспроводных устройств, должен обеспечить повышенную конфиденциальность с помощью четырех новых возможностей.

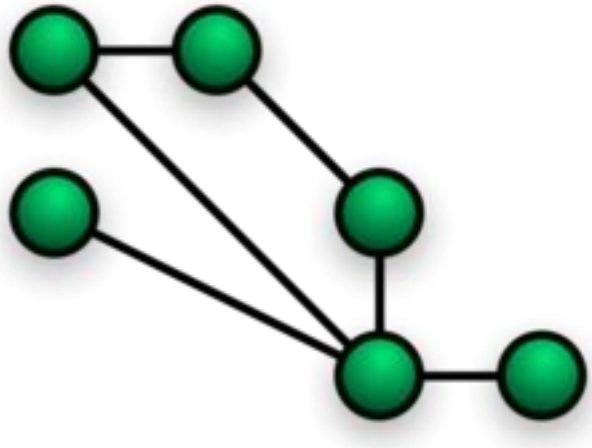
1. Протокол WPA3 укрепляет конфиденциальность пользователей в открытых сетях посредством индивидуального шифрования данных. Можно шифровать соединение между каждым устройством и точкой доступа.
2. Внедрена защита от атаки методом «грубой силы», не позволяющая хакерам совершать несколько попыток входа в систему с использованием часто используемых паролей. Защитный механизм работает через блокировку процесса аутентификации после того, как произошло несколько безуспешных попыток авторизации.

3. Внедрена упрощенная настройка для IoT-устройств. В WPA3 есть возможность использовать Wi-Fi устройства, которые размешены вблизи друг от друга, как конфигурационную панель для других устройств. Так, пользователь сможет задействовать телефон или планшет для того, чтобы настраивать параметры Wi-Fi WPA3 на устройствах, не имеющих экрана.
4. Внедрен модернизированный криптографический стандарт для сетей Wi-Fi, так называемый «192-разрядный пакет безопасности». Он будет ориентироваться на Commercial National Security Algorithm (CNSA) Suite, созданный Комитетом по системам национальной безопасности (Committee on National Security Systems). Данное решение предназначается в первую очередь для сетей с более высокими требованиями безопасности, такими как правительственные, оборонные и промышленные организации

Поскольку аппаратное обеспечение должно быть сертифицировано Wi-Fi Alliance для использования протокола безопасности WPA3, новый стандарт безопасности не будет внедрён в одночасье. Производителям устройств может потребоваться несколько месяцев. Более подробная информация о WPA3 будет опубликована позднее.

Лекция 9. Mesh сети.

Ячеистая топология



Ячеистая топология — сетевая топология компьютерной сети, построенная на принципе ячеек, в которой рабочие станции сети соединяются друг с другом и способны принимать на себя роль коммутатора для остальных участников. Данная организация сети является достаточно сложной в настройке, однако при такой топологии реализуется высокая отказоустойчивость. Как правило, узлы соединяются по принципу «каждый с каждым». Таким образом, большое количество связей обеспечивает широкий выбор маршрута следования трафика внутри сети — следовательно, обрыв одного соединения не нарушит функционирования сети в целом.

Беспроводные ячеистые сети

Сеть беспроводных устройств, функционирующая по принципам ячеистой топологии, называется беспроводной ячеистой сетью.

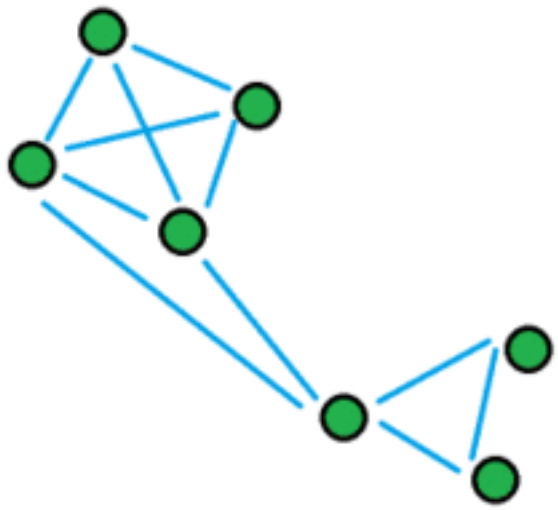
Ячеистые сети изначально разрабатывались в военных целях и, как правило, являются беспроводными. За последнее время размер устройств, стоимость, а также их энергопотребление снизились, и стало возможным добавление нескольких радиомодулей на один узел. Вследствие чего каждая ячейка получила возможность одновременно выполнять несколько полезных функций, таких как клиентский доступ, сканирование, требуемое для высокоскоростных передач в мобильных приложениях и прочие.

Для разработки такого типа сетей полезными оказываются знания методов теории игр, которые помогают анализировать стратегии выделения ресурсов и построения маршрутов в ячеистой топологии.

Узлы первых беспроводных ячеистых сетей представляли из себя устройства, способные работать только в режиме полудуплекс.

Позднее, с развитием радиомодулей, стало естественным осуществление приема и передачи одновременно на разных частотах или CDMA-каналах, что резко подтолкнуло развитие сетей с ячеистой топологией.

Общие особенности



Самовосстановление и самоадаптация

- **«Интеллектуальность» сети**

Является одной из ключевых особенностей беспроводной ячеистой сети. «Интеллектуальность» означает, что при подключении каждая точка автоматически получает информацию обо всех других точках доступа в сети и «выясняет» свою роль. Такое поведение исключает необходимость постоянного администрирования и способствует быстрому развертыванию.

- **Самовосстановление и самоадаптация**

Как можно понять из предыдущего пункта — как только сеть включена и начинает функционировать, то каждое устройство автоматически определяет состояние соседей и свою роль в общей топологии. Поэтому, при выходе из строя одного из узлов, сеть способна перенаправить данные — то есть переопределить маршруты автоматически.

- **Быстрое и недорогое развертывание**

Развертывание ячеистой сети не требует дорогостоящей инфраструктуры и прокладки кабелей. Кроме того, в силу способностей к самовосстановлению и самоадаптации — данная сеть является экономной в эксплуатации.

Организация сети

Беспроводные ячеистые сети — первый шаг в направлении экономически эффективных и динамических сетей с высокой пропускной способностью. Такая топология, по сути, является сетью маршрутизаторов, лишенной проводов между узлами. Беспроводная ячеистая сеть построена на Peer radio-устройствах, которые не требуют кабельного соединения, необходимого для традиционных беспроводных точек доступа. Mesh-топология позволяет передавать данные на большие расстояния путём разбиения длинного маршрута на серию коротких переходов между узлами — хопов/hops. Промежуточные узлы не только усиливают сигнал, но и совместно передают его от точки А до точки В — осуществляют переадресацию, основываясь на их знании о сети в целом. Другими словами — каждый узел осуществляют маршрутизацию. Такая архитектура, при тщательной разработке и анализе, может обеспечить высокую пропускную способность, спектральную эффективность и экономическое преимущество в зоне покрытия.

Топология беспроводной ячеистой сети относительно постоянна. Только в случаях внезапного отключения или добавления новых узлов могут быть инициированы процессы изменения структуры сети. Маршрут движения трафика, будучи сформированным большим числом конечных пользователей — редко меняется. Практически весь трафик в топологии ячеистой сети либо направлен через шлюз, либо исходит из него, в то время как в беспроводных ad-hoc сетях трафик течет между произвольной парой узлов.

Данный тип топологии может быть децентрализованным или централизованным — в зависимости от присутствия в сети главного сервера, оба подхода относительно недороги, надежны и отказоустойчивы, так как задача каждого узла — передача трафика только до следующего узла сети. Каждое устройство выполняет функции маршрутизатора по передаче данных от соседних узлов к удаленным участникам сети, для достижения которых недостаточно одного перехода. В результате получена сеть, способная покрывать огромные расстояния, не теряя своей устойчивости. Надежность Mesh-топологии обеспечивается так же тем, что каждый узел соединен с несколькими соседями. Это значит, что при выбывании узла из топологии из-за неисправностей устройства или по каким-либо другим причинам, его соседи смогут быстро перестроить маршрут для трафика, используя свои протоколы маршрутизации.

Области применения

Ячеистые сети можно применить для решения широкого спектра задач — наблюдения за полем боя, телеметрия гоночного автомобиля в реальном времени, настройка сети в условиях неблагоприятной окружающей среды и пр. В зависимости от поставленной задачи, можно настроить поведение ячеистой структуры наиболее подходящим образом. Такая гибкость обеспечивается большим количеством разнообразных возможностей и особенностей данной топологии, которые можно комбинировать произвольным способом. Например, одной из наиболее полезных для применения особенностей ячеистой сети является возможность реализации протокола VoIP поверх ячеистой топологии, используя схему QoS. Такая реализация позволяет поддерживать локальные телефонные разговоры за счет ресурсов сети. В число устройств могут входить как стационарные, так и мобильные, что, опять же, обеспечивает легкость развертывания и гибкость настройки при решении конкретной задачи.

Функционирование

Принцип во многом напоминает способ перемещения пакетов в проводной сети — данные перемещаются от одного устройства к другому до тех пор, пока пакет не достигнет назначенного получателя. Это обеспечивается алгоритмами динамической маршрутизации, встроенным в каждое устройство. Для реализации таких динамических протоколов необходимо, чтобы все устройства сети регулярно обменивались маршрутной информацией между собой. После чего каждый узел определяет, что он должен сделать с полученной информацией — либо передать пакет на следующее устройство, либо сохранить его, согласно указаниям протокола. Кроме того, алгоритмы маршрутизации должны соответствовать требованию о кратчайшем маршруте — то есть строить наиболее подходящий и эффективный маршрут до узла назначения.

Коммерческие mesh-маршрутизаторы

Цифровые радиоприемники ZigBee встраиваются в некоторые устройства бытовой техники, включая те, которые функционируют от батареек. ZigBee-радиомодули произвольным образом организуются в ячеистую сеть, используя AODV-маршрутизацию; передача и прием синхронизированы. Это означает, что радиомодули могут быть выключены большую часть времени для экономии потребления энергии.

В начале 2007 года фирма Meraki запустила свой проект — беспроводной мини-mesh-маршрутизатор. Данная разработка — пример беспроводной ячеистой сети с заявленной скоростью обмена данными 50 Мбит/сек. Протокол беспроводной связи 802.11 был оптимизирован в устройствах Meraki для передачи данных на большие расстояния, что обеспечило покрытие на расстояния более 250 метров.

Использование

Связь в регионах с неразвитой инфраструктурой

Ноутбуки программы One Laptop Per Child используют беспроводные ячеистые сети для предоставления учащимся возможности обмениваться файлами и подключаться к сети интернет даже при отсутствии рядом каких-либо средств физического подключения, таких как кабели, мобильные телефоны и пр.

В сельском районе Каталонии в 2004 году была разработана сеть Guifi.net — как ответ на недоступность широкополосного интернета в регионе, ввиду того, что местные интернет-провайдеры практически не предоставляли данного вида услуг. На сегодняшний день в этой сети существует более 30000 узлов и, благодаря peer to peer соглашению, данная сеть остается открытой, свободной и нейтральной с обширными возможностями резервирования.

Связь в крупных корпоративных средах

Решение проблемы «бутылочного горлышка». У беспроводных сетей, предназначенных для крупных корпоративных сред есть существенный недостаток — так называемый эффект «Бутылочного горлышка», который можно наблюдать при использовании большого количества точек доступа. Другими словами: при большом числе подключений наблюдается резкое снижение пропускной способности сети. Это объясняется особенностями точек доступа стандарта 802.11, которые предоставляют разделяемую среду, где в данный момент времени только одна из них может вести передачу данных.

Таким образом, в традиционной сети все клиенты подключаются к единственной точке доступа, имеющей выход в интернет. В сети с ячеистой топологией любое устройство способно выступать как в роли маршрутизатора, так и точки доступа. Такой принцип позволяет при большой нагрузке на устройство перенаправить данные на ближайшего, менее загруженного соседа.

Связь на массовых мероприятиях

3 июня 2006 года, в Кембридже, ячеистая сеть была использована на традиционном музыкальном фестивале «Strawberry Fair» для запуска мобильных сервисов live-телевидения, радио и интернета для, приблизительно, 80000 человек.

Военное дело

Беспроводные ячеистые сети на сегодняшний день используются силами армии США для обеспечения соединения компьютеров — в основном, защищенных ноутбуков, при проведении полевых операций.

Энергетика

Установленные на конечных узлах электросчетчики собирают общую информацию, передавая измеренные показания от одного к другому, а в итоге — в центральный офис для выставления счета клиенту. Такая организация позволяет исключить необходимость использования человеческого труда для снятия показаний приборов, а также избавиться от кабелей для подключения счетчиков.[5]

Спутниковая связь

66 спутников созвездия Иридиум функционируют как единая mesh-сеть с беспроводными соединениями между соседними спутниками. Звонок между двумя спутниковыми телефонами передается через ячеистую сеть от одного спутника до другого внутри «созвездия» без необходимости взаимодействия со станциями связи на Земле. Это обеспечивает более короткие пути следования сигнала, снижает задержку при разговоре, а также позволяет «созвездию» функционировать, используя гораздо меньшее количество земных спутниковых станций, чем потребовалось бы для 66 традиционных спутников связи.

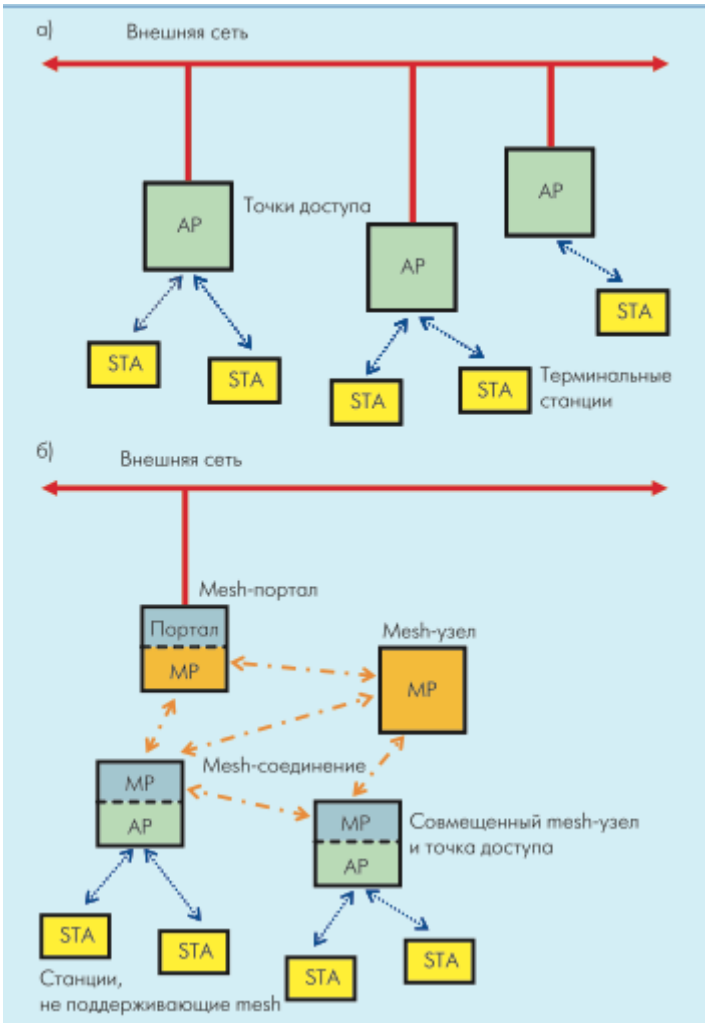
Mesh-сети стандарта IEEE 802.11s

Опубликованный двадцать лет назад стандарт локальных сетей беспроводного доступа IEEE 802.11 (беспроводный Ethernet) оказался настолько удачным, что продолжает развиваться до сих пор. Ему уже давно стало тесно в рамках сотен метров, отведенных локальным сетям. На основе оборудования 802.11 строятся – и вполне успешно – как персональные сети, так и сети городского масштаба. Одним из направлений в развитии стандарта стала технология mesh-сетей, которую разрабатывают в рамках грядущего стандарта IEEE 802.11s. Это тот случай, когда потребности рынка и сами производители обгоняют усилия по стандартизации – стандарта пока нет (но вскоре ожидается), а оборудование и сети уже строятся.

Mesh-сети – новый перспективный класс широкополосных беспроводных сетей передачи мультимедийной информации, который в ближайшие годы найдет широкое применение при построении локальных и распределенных городских беспроводных сетей (альтернатива WiMAX), при разворачивании мультимедийных сенсорных сетей и т.д. Одним из главных принципов построения mesh-сети является принцип самоорганизации архитектуры, обеспечивающий такие возможности, как реализацию топологии сети "каждый с каждым"; устойчивость сети при отказе отдельных компонентов; масштабируемость сети – увеличение зоны информационного покрытия в режиме самоорганизации; динамическую маршрутизацию трафика, контроль состояния сети и т.д. Mesh-сети могут быть стационарными или мобильными. В последнем случае все или часть узлов со временем могут менять свое местоположение. В мобильных сетях в качестве узлов могут использоваться карманные ПК, мобильные телефоны и другие персональные устройства.

Протокол IEEE 802.11s

В существующих сетях стандарта 802.11 терминальные (абонентские, конечные) станции (STA) связаны с точками доступа (Access Point – AP) и могут взаимодействовать только с ними. AP имеют выход в другие сети (например, Ethernet), но не могут обмениваться информацией друг с другом (рис.1а). В meshсети, помимо терминальных станций и точек доступа, присутствуют особые устройства – узлы mesh-сети (Mesh Point – MP), способные взаимодействовать друг с другом и поддерживающие mesh-службы (рис.1б). Одно устройство может совмещать несколько функций. Так, узлы mesh-сети, совмещенные с точками доступа, называются точками доступа mesh-сети (Mesh Access Point, MAP). Порталы mesh-сети (Mesh Point Portal, MPP), являясь MP, соединяют mesh-сеть с внешними сетями. Таким образом, mesh-сеть с точки зрения других устройств и протоколов более высокого уровня функционально эквивалентна широковещательной Ethernet-сети, все узлы которой непосредственно соединены на канальном уровне.



Отметим, что изменения в стандарте IEEE 802.11s практически не затрагивают физический уровень. Все нововведения относятся к MAC-подуровню канального уровня. Кроме того, в стандарте 802.11s рассматриваются вопросы маршрутизации пакетов в рамках mesh-сети (фактически – сетевой и транспортный уровень модели OSI), что выходит за изначальные рамки IEEE 802.11. Вопросы маршрутизации пакетов в meshсетях мы рассмотрим в следующей публикации, сосредоточившись в данной работе на особенностях MAC-уровня.

Структура пакетов MAC-уровня в mesh-сети аналогична стандартному формату пакетов сетей 802.11. Формат заголовка MAC-пакета в mesh-сети полностью соответствует MAC-заголовку пакета данных, определенному в стандарте IEEE 802.11 (за исключением поля HT Control (High Throughput Control), предназначенного, видимо, для поддержки оборудования стандарта IEEE 802.11n. Первые три поля заголовка и поле контрольной суммы FCS присутствуют во всех пакетах MAC-уровня.

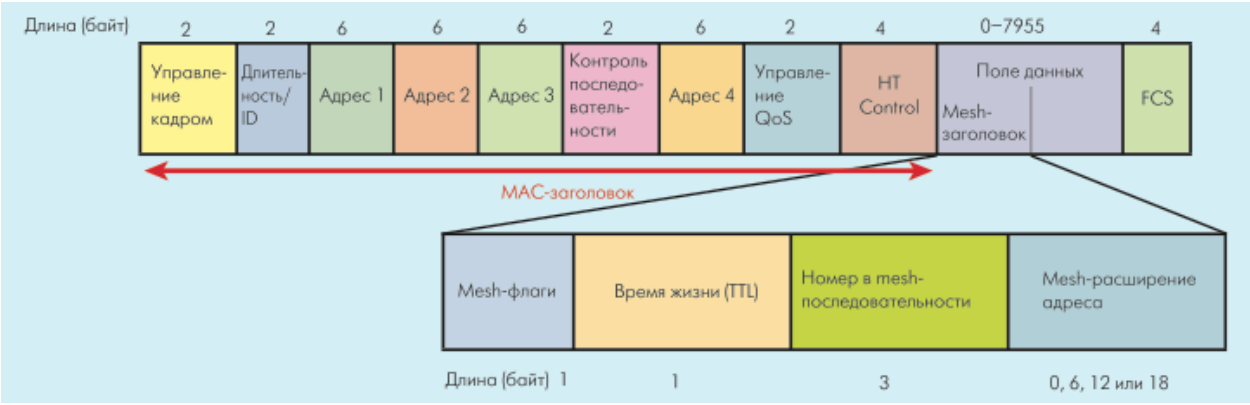
Отличие MAC-пакетов 802.11s заключается в наличии mesh-заголовка в начале поля данных. Этот заголовок присутствует в пакетах данных тогда и только тогда, когда они передаются от mesh-узла к mesh-узлу по установленному между ними соединению, он так же присоединяется к одному из типов (Multihop Action) управляющих пакетов.

Mesh-заголовок содержит четыре поля. Байт mesh-флагов регулируют обработку mesh-заголовка. Пока используются только первые два бита, которые просто определяют размер расширенного mesh-адреса. Поле "время жизни пакета в mesh-сети" (Mesh Time To Live – MTL) содержит оставшееся максимальное число шагов между узлами, которое может совершить пакет в mesh-сети. Таким образом ограничивается время жизни пакета при многошаговой пересылке, что помогает бороться с образованием циклических маршрутов. Номер пакета в последовательности (Mesh Sequence Number) пресекает появление дубликатов пакетов при широковещательной и многоадресной посылке.

Поле расширения mesh-адреса (Mesh Address Extension) может включать дополнительные адреса (Адрес 4, Адрес 5 и Адрес 6, каждый по 6 байт), что позволяет mesh-пакетам содержать до 6 адресов. Адрес 4 используется в управляющих пакетах типа Multihop Action (при эстафетной передаче в mesh-сети), поскольку в формате управляющих пакетов MACуровня поле Адрес 4 отсутствует. Адреса 5 и 6 могут служить для передачи адресов конечных отправителя и получателя, если они оба или один из них не являются MP. Это возможно, если узлы вне mesh-сети общаются через mesh-сеть. Возможен и случай, когда два MP-устройства взаимодействуют через корневой узел mesh-сети, т.е. используются два отдельных mesh-пути (от отправителя до корневого узла и от корневого узла до получателя).

MDA-резервирование

Детерминированный доступ в mesh-сети (Mesh Deterministic Access – MDA) – это опциональный механизм, позволяющий получать доступ к среде в заранее зарезервированные временные интервалы. Это снижает конкуренцию доступа к среде передачи, что позволяет существенно увеличить вероятность своевременной доставки данных, чувствительных к задержкам (аудио и видеопотоки, данные с высоким приоритетом и т.п.).



Формат MAC-кадра с Mesh-заголовком

MDA-соединение может быть установлено только между станциями, поддерживающими данный механизм. MDA-резервирование задает интервалы, в течение которых поддерживающие MDA станции не пытаются передавать пакеты, чтобы не мешать передаче данных по зарезервированному каналу.

Создание MDA-соединения инициируется узлом-источником, а принимается или отклоняется узлом-адресатом данных. Для установления MDA-соединения устройство выбирает интервалы времени, не занятые другими MDA-соединениями, о которых ему известно. Если резервирование нового соединения вызывает превышение допустимого числа MDAсоединений для соседей данного узла, то устройство отказывается от создания соединения.

При установлении MDA-соединения узел направляет соответствующий запрос узлу-адресату, указав, в какие моменты времени и какой длины интервалы он хочет использовать. Получатель запроса выполняет аналогичные проверки о допустимости создания соединения с запрошенными параметрами и шлет ответ – положительный или отрицательный. Если выбранные узлом-источником временные интервалы пересекаются с другими MDA-соединениями, о которых известно получателю, он может в ответе предложить альтернативные интервалы времени. Для разрыва MDA-соединения получатель или отправитель могут послать специальный информационный элемент (MDAOP Set Teardown information element).

Все устройства, которые знают о существовании MDA-резервирований, обязаны периодически сообщать о них своим соседям (рекламировать) посредством либо специальных информационных элементов (MDAOP Advertisements information element), включенных в биконы, либо используя специальные служебные кадры (MDA action frame). Узлы, поддерживающие механизм MDA, хранят список всех резервирований, о которых узнают из рекламных сообщений и в которых участвуют сами (передают или принимают).

Важно отметить, что даже при зарезервированном MDAинтервале доступ к среде передачи происходит на конкурентной основе. При этом учитывается категория трафика, который пытается передать станция, для чего используется

механизм доступа к каналу с поддержкой дифференцированного качества обслуживания (Enhanced Distributed Channel Access, EDCA).

Установка и управление соединениями в IEEE 802.11s

Совместимость устройств от разных производителей в одной сети обеспечивает концепция профилей. Профиль содержит собственно идентификатор профиля, идентификатор протокола маршрутизации и идентификатор метрики протокола маршрутизации. Устройство может поддерживать несколько профилей работы, но лишь один из них может быть активным. Обязательный для всех устройств стандарта 802.11s профиль использует гибридный беспроводной mesh-протокол маршрутизации (HWMP, Hybrid Wireless Mesh Protocol) и метрику времени передачи в канале (Airtime Link Metric).

Механизм установки соединений основан на периодической посылке стандартного сообщения "открыть соединение". В ответ на него может быть получено сообщение "подтверждение соединения" или "закрытие соединения". Соединение между двумя соседними MP считается

установленным тогда и только тогда, когда оба MP послали друг другу команды "открыть соединение" и ответили подтверждением соединения (в любой последовательности). Для каждого установленного соединения предусмотрено время жизни, в течение которого оно должно быть использовано либо подтверждено.

синхронизация и биконы в IEEE 802.11s

Стандарт IEEE 802.11 поддерживает два режима работы беспроводных сетей: hot spot и ad hoc. В режиме hot spot одна из станций работает в качестве точки доступа, и данные могут передаваться только между точкой доступа и другими станциями сети. В режиме ad hoc передача возможна между любыми двумя станциями.

В режиме hot spot точка доступа регулярно рассылает специальные кадры – биконы (beacon), главная цель которых заключается в синхронизации часов станций и информировании о сервисах и режимах работы, которые поддерживает точка доступа. Биконы содержат специальное поле Timestamp, в котором записано время, когда первый бит бикона оказывается переданным через радиоинтерфейс. На основании этого значения происходит синхронизация часов всех станций. Синхронизация внутренних часов важна как для физического, так и для канального уровней. Например, в режиме модуляции с расширением спектра методов частотных скачков (FHSS) необходимо гарантировать, что переключение всех станций на новую частоту происходит одновременно. Также синхронизация важна для работы режима энергосбережения.

В режиме ad hoc биконы выполняют ту же функцию, что и в режиме hot spot. Но процесс передачи бикона является распределенным, т.е. в нем участвуют все станции. Станция, которая организует сеть ad hoc, задает серию моментов времени, которые называют ожидаемым временем передачи бикона (Target Beacon Transmission Time, TBTT). Последовательные моменты TBTT отделены друг от друга равными интервалами времени – бикон-интервалами. В каждый момент TBTT начинается так называемое ATIM-окно (Announcement Traffic Indication Message – сообщение уведомления о трафике), во время которого могут быть переданы только биконы или ATIM-кадры (используются механизмом энергосбережения), в то время как трансляция других пакетов запрещена для снижения вероятности коллизии.

Передача бикона основана на том же механизме конкурентного доступа с контролем несущей, что и при передаче данных. В момент TBTT каждая из станций замораживает счетчик времени отсрочки передачи данных и инициализирует таймер передачи бикона случайно выбранным числом слотов (единица дискретного времени в сети 802.11), равномерно распределенным в интервале от нуля до некоей константы (2·aCWmin). Если среда передачи не занята в течение слота, станция уменьшает значение таймера на единицу. Если одна из станций начинает передачу, другие станции замораживают свои таймеры на время передачи плюс интервал времени DIFS. Если происходит коллизия, т.е. более одной станции передают одновременно, то вместо времени DIFS используется более длинный интервал EIFS. Станция начинает передачу бикона в момент, когда значение ее таймера становится равным нулю. При получении бикона от любой из станций все остальные станции отменяют передачу своих биконов.

Алгоритм посылки биконов, остающийся неизменным в течение десяти лет существования стандарта IEEE 802.11, используется и в стандарте IEEE 802.11s. Именно этот механизм поддерживает глобальную синхронизацию сети, когда все устройства работают по единому времени, привязанному к ожидаемому времени передачи бикона.

Узлы mesh-сети MP могут, но не обязаны поддерживать глобальную синхронизацию в сети. Соответственно, они подразделяются на синхронные и асинхронные MP. Асинхронные MP передают биконы подобно точкам доступа в сетях hot spot. При этом каждая станция поддерживает независимо от других станций серию моментов TBTT и не подводит свои часы при получении биконов. Синхронные MP стараются поддерживать общее для всех время Mesh TSF.

Синхронные MP передают биконы по тому же алгоритму, что и в сетях ad hoc, за исключением следующего аспекта. Если MP получило бикон от соседнего устройства mesh-сети, оно может отменить запланированную передачу собственного бикона, но не обязано это делать, как в ad hoc сети. В mesh-сети одного бикона от случайно выбранного MP может оказаться недостаточно.

По сравнению с сетями ad hoc, mesh-сети поддерживают дополнительные mesh-сервисы, и биконы ответственны за их поддержку. Например, механизм детерминированного доступа MDA использует биконы для передачи в них специального информационного элемента MDAOP Advertisements с рекламой MDA-резервирований. Этот и другие дополнительные информационные элементы делают биконы в mesh-сети более индивидуальными, по сравнению с биконами в сетях ad hoc, которые разнятся только значением временной метки (поля бикон-кадра, описывающие возможные режимы работы станции, не меняются в течение всего времени существования сети ad hoc). Потому важно, чтобы каждое MP отправляло свой бикон как можно чаще.

В дополнение к алгоритму рассылки биконов, используемому в сетях hot spot и ad hoc, в первой версии 802.11s/D1.00 было введено понятие распространителя биконов (точки биконов) – Beacon Broadcaster (BB). Когда BB выбран, оставшиеся MP биконы не передают. Роль BB периодически передается от одного MP другому. Однако в mesh-сети некоторые станции скрыты друг от друга, что приводит к появлению нескольких BB, и задача ротации BB становится слишком сложной. В связи с этим в более поздних версиях стандарта meshсетей использование BB исключено.

В текущей версии IEEE 802.11s сделан еще один шаг в сторону от использования принципа глобальной синхронизации mesh-сети. Дело в том, что в mesh-сети глобальная синхронизация требует больших издержек: размер ATIM-окна должен быть увеличен по сравнению с сетями ad hoc, чтобы уместить возможно большее число биконов MP. Поэтому вместо поддержки глобальной синхронизации MP могут лишь поддерживать синхронизацию попарно. При этом MP рассылают биконы независимо, без привязки к единому времени TBTT и единому ATIM-окну. Издержки сети при этом могут уменьшиться, но, по-видимому, качество ее работы снизится: без глобальной синхронизации сети трудно защитить биконы от коллизий с данными, а значит, нельзя обеспечить качество обслуживания и эффективную работу режима сохранения энергии.

Работа над дополнением к стандарту IEEE 802.11s еще не завершена. Пока не ясно, какая парадигма синхронизации будет принята в mesh-сети. Мы уверены, что глобальная синхронизация mesh-сети и алгоритм рассылки биконов, похожий на алгоритм в сетях ad hoc, позволят обеспечить качество обслуживания (QoS) в рамках всей mesh-сети, а также применять эффективные методы энергосбережения, все более востребованные на рынке телефонов, коммуникаторов и т.п. В сети без глобальной синхронизации обеспечение QoS представляется чрезвычайно трудной, если вообще разрешимой задачей. Поэтому сегодня основное внимание уделено изучению алгоритма рассылки биконов синхронными MP, как они описаны в первой завершенной версии стандарта IEEE 802.11s/D1.00.

Энергосбережение в IEEE 802.11s

Режим энергосбережения в mesh-сетях является опциональным. Так, MAP-узлы всегда активны, поскольку в любой момент к ним могут обратиться устройства, не поддерживающие 802.11s и соответствующий режим энергосбережения. Однако для устройств с автономным питанием (разного рода датчики, ноутбуки, телефоны и т.п.) сбережение энергии – актуальная задача.

Узлы сети обязаны сообщать о своей способности поддерживать спящий (энергосберегающий) режим. Для этого используется информационное поле возможностей (capability information field) в биконах и в ответах на пробные пакеты. В этом же поле сообщается, что узел находится в режиме энергосбережения либо имеет связь с узлом, который пребывает в этом режиме. Если устройство, желающее работать в режиме энергосбережения, видит, что его сосед не поддерживает эту возможность, то оно может либо не устанавливать соединения с таким устройством, либо установить его, но отказаться от перехода в режим энергосбережения. Узел не может переходить из активного режима в режим энергосбережения (и обратно), пока не проинформирует все устройства, с которыми у него установлено соединение, о своем желании переключиться. Для информирования соседей о смене режима энергосбережения используются пустые пакеты данных (null-data frame).

Узел в спящем режиме периодически просыпается, чтобы получить биконы от своих соседей либо послать свои. Узел просыпается по крайней мере один раз за так называемый DTIM-интервал (delivery traffic indication message – сообщение о наличии пакетов для станции) и остается активным в промежутке времени окна ATIM (Announcement Traffic Indication Message – окно для сообщений о трафике). Все узлы mesh-сети, поддерживающие режим энергосбережения, откладывают посылку пакетов, предназначенных для устройств в спящем режиме (в том числе широковещательных и многоадресных) и отправляют их только в назначенный промежуток времени. О наличии этих пакетов узел-источник сообщает в сообщении Mesh TIM в биконе или в передаваемом ATIM-кадре, следующем за DTIM-биконом. Устройства, находящиеся в режиме энергосбережения, слушают такие сообщения о наличии для них данных, и если обнаруживают их, остаются активными после ATIM-окна. Если узел получил широковещательный или многоадресный пакет, то он остается активным до тех пор, пока не получит пакета, в котором поле о наличии данных (More Data field) говорит о том, что адресованных ему данных более не осталось, либо Mesh TIM элемент с той же информацией.

Спящие узлы могут проснуться в любой момент времени, если у них в очереди оказывается пакет на передачу. В этом случае такой узел остается бодрствовать, по крайней мере, до следующего момента времени TBTT.

Режим энергосбережения отличается для синхронных и асинхронных MP. Так, асинхронные MP используют свои собственные значения ATIM и DTIM, а все узлы, с которыми они установили соединение, сохраняют эти параметры для дальнейшей работы. Синхронные же MP, присоединяясь к сети, используют общие ATIM и DTIM значения, которые они получают в биконах от соседей, в этом случае все спящие устройства в сети будут просыпаться одновременно.

оборУдование для MEsh-сетей

Cisco Systems представила беспроводную платформу Cisco Aironet 1520 Series, включающую в себя точку доступа mesh-сети внешнего исполнения Cisco Aironet 1522, на базе которой и строится mesh-сеть. При этом используется закрытый фирменный протокол маршрутизации Adaptive Wireless Path Protocol (AWPP). Логика протокола скрыта, однако по косвенным данным можно предположить, что он базируется на одной из версий протокола HWMP, работающего в проактивном режиме. Управлением и мониторингом сети занимается специальное устройство – контроллер беспроводной сети Cisco Wireless LAN Controller. Компания рекомендует использовать в mesh-сетях контроллеры серии 4400. Этот контроллер также может служить центром безопасности сети, поскольку включает в себя RADIUS сервер и поддерживает ряд других служебных сервисов.

Контроллер и устройства сети обмениваются между собой служебной информацией по протоколу управления Lightweight Access Point Protocol (LWAPP). Открытая версия этого протокола редактируется и обсуждается на сайте открытого международного сообщества IETF (Internet Engineering Task Force).

Одна из самых известных в мире фирм в области mesh-сетей – компания Tropos Networks. Она, в тесном сотрудничестве с фирмой Juniper, уже реализовала свыше 500 проектов (в США и по всему миру) на основе своего решения MetroMesh. Ярким примером может служить уже год как работающая сеть Google WiFi, объединяющая более 400 маршрутизаторов в опорной сети, покрывающая более 30 км2 и 25 тыс. домов для обслуживания 15 тыс. пользователей. Данного результата удалось достичь благодаря разработке и использованию специального протокола маршрутизации Predictive Wireless Routing Protocol (PWRP), способного работать в больших сетях без потери пропускной способности.

Примечательно и решение компании Nortel – точка доступа Wireless Access Point 7220. Именно на его основе построена московская беспроводная сеть Golden WiFi, которая в 2007 году была признана крупнейшей городской сетью WiFi в мире. Для мониторинга и управления сетью в данном решении используется специальный графический пользовательский интерфейс ENMS, который базируется на протоколе SNMP.

Компания Firetide анонсировала точки доступа mesh-сети HotPoint серии 4000. Эти устройства осуществляют полностью прозрачный переход между существующей проводной и беспроводной mesh-сетью.

Свое решение для mesh-сетей представила и широко известная фирма Proxim. Серия устройств ORiNOCO Wi-Fi Mesh Series примечательна тем, что использует специальный протокол ORiNOCO Mesh Creation Protocol (OMCP), позволяющий использовать один и тот же беспроводной интерфейс как для формирования транспортной mesh-сети, так и для организации доступа пользователей к беспроводной сети.

Первой отечественной реализацией оборудования meshсетей внешнего исполнения является аппаратно-программный комплекс, разработанный Институтом проблем передачи информации РАН им. А.А.Харкевича (ИППИ РАН), на базе серийно выпускаемого комплекса “Рапира” [6]. В этом оборудовании в качестве базового протокола маршрутизации используется протокол HWMP (в его текущей редакции), а также оригинальный протокол маршрутизации, разработанный в ИППИ РАН, позволяющий производить полностью прозрачный переход между существующей проводной и беспроводной mesh-сетью. Кроме того, это оборудование использует контроллер беспроводной сети, обмен данными с которым происходит по протоколу LWAPP.

Преимущества и недостатки

Данная технология решает следующие проблемы:

- Позволяет быть независимыми от провайдеров
- Вы можете сами построить свою сеть с шлю... Wi-Fi роутерами и маршрутизацией
- Для подключения к сети вам не нужно производить никаких сложных действий *(при условии, если сеть самонастраиваемая)*
- Каждый новый клиент, который подключился к сети, увеличивает ёмкость сети
- Понятие «бесплатный Wi-Fi дома» меняется на «бесплатный Wi-Fi везде»
- Если произошло стихийное бедствие, то с помощью Mesh сети можно быстро построить сеть на месте пришествия для связи, при поддержке из вне — соединить её с глобальной сетью

Плюсы и минусы Mesh сетей

Плюсы:

- Независимость от провайдера, режима, власти
- При стихийных бедствиях позволяет иметь сеть на месте происшествия, хотя возможно и отрезанную от глобальной части
- Некоторые современные протоколы для строительства Mesh сетей гарантируют шифрование всего трафика проходящего через сеть (cjdns)

- Динамическая, авто-конфигурируемая маршрутизация
- Возможность объединять mesh сети через обычный интернет *(cjdns)*

Минусы:

- Первоначальный запуск Mesh сети очень сложен
- Эффективная работа достигается когда в сети много участников
- Из-за отсутствия привычных пользователям ресурсов Mesh сеть может отпугивать новичков
- Негарантированная ширина канала
- Негарантированное качество связи