# 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

* + 1. **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.

* + 1. **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).

* + 1. **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.

* + 1. **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.

* + 1. **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 |

* + 1. **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);

С-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.

* + 1. **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).

* + 1. **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.

* + 1. **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.

* + 1. **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»).

* + 1. **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.

* + 1. **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**

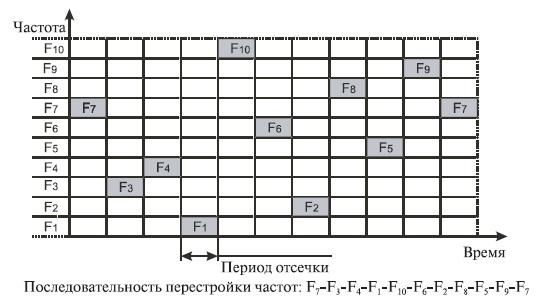
Изначально метод расширенного спектра создавался для разведывательных и военных целей. Основная идея метода состоит в том, чтобы распределить информационный сигнал по широкой полосе радиодиапазона, что в итоге позволит значительно усложнить подавление или перехват сигнала. Первая разработанная схема 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.

* + - * 1. **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.

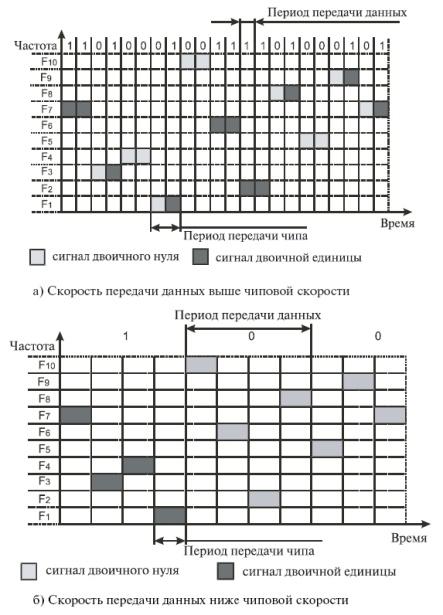
В течение фиксированного интервала времени передача ведется на неизменной несущей частоте.



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](http://www.intuit.ru/department/network/wifi/1/6.html#image.1.11%23image.1.11)); в противном случае мы имеем дело с - быстрым расширением спектра ([рис.б](http://www.intuit.ru/department/network/wifi/1/6.html#image.1.11%23image.1.11)).



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.

* + - * 1. **Прямое последовательное расширение спектра (Direct Sequence Spread Spectrum - DSSS)**
        2. **(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 **Ci**.

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 (5В8)h. Если передатчик использует эту последовательность, то передача трех битов 110 ведет к передаче следующих битов:

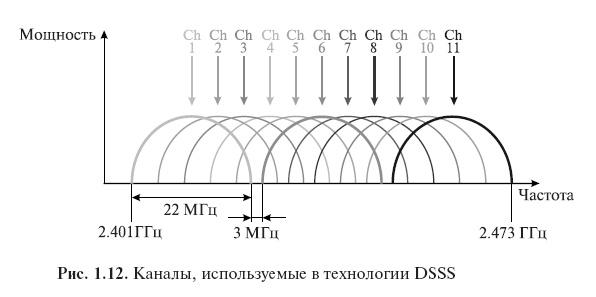
10110111000 10110111000 01001000111.

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 |  |  |
|  |  |  | Х |  |  | Х | Х |  | Х | Х |  |  |
|  | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 |  |
|  |  | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 |
|  |  |  |  | Х |  |  | Х | Х |  | Х | Х |  |

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.



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 Ts, то период сигнала OFDM будет равен NTs. Это позволяет существенно снизить влияние межсимвольных помех. При проектировании системы N выбирается таким образом, чтобы величина NTs 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).

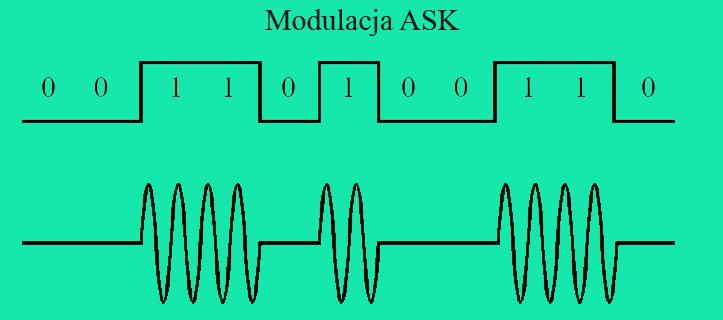
## Виды манипуляций

Существуют следующие типы манипуляций:

* Частотная манипуляция
* Фазовая манипуляция
* Амплитудная манипуляция
* Квадратурная амплитудная манипуляция

### Амплитудная манипуляция

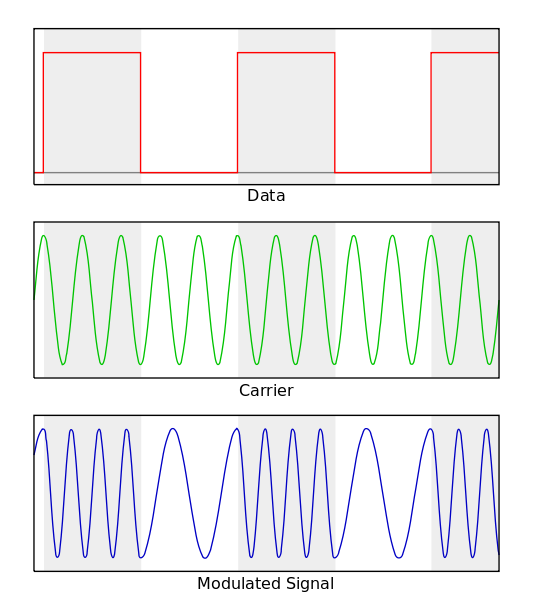
Амплитудная манипуляция (АМн; англ. amplitude shift keying (ASK) — изменение сигнала, при котором скачкообразно меняется амплитуда несущего колебания.



### 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.

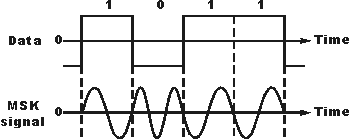
**Частотная манипуляция с минимальным сдвигом** (англ. *Minimal Shift Keying (MSK)*) представляет собой способ модуляции, при котором не происходит скачков фазы и изменение частоты происходит в моменты пересечения несущей нулевого уровня. MSK уникальна потому, что значение частот соответствующих логическим «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.

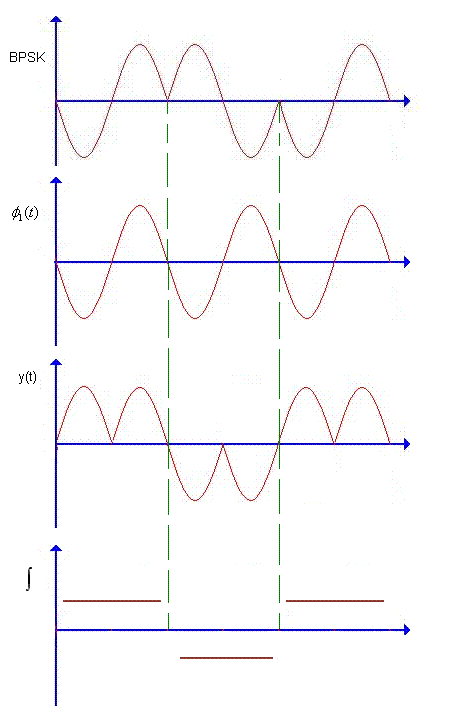
Преимущество данного вида модуляции в том, что он имеет минимальный уровень излучения на боковых и зеркальных частотах, то есть не мешает другим пользователям эфира. Плотность информации — 1 бит на символ или на герц. Данный вид модуляции, как и MSK, относится к частотным видам модуляции с непрерывной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

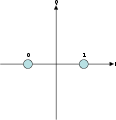
Модулирующий сигнал получается путём преобразования информационного потока из вида 0/1 в вид −1/+1. Затем −1/+1 сигнал фильтруется таким образом, что сформированный +1/-1 прямоугольный сигнал преобразуется в сигналы имеющие форму гауссовского импульса. Далее полученный сигнал подается на ЧМ модулятор 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.

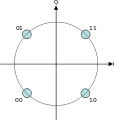
### Фазовая манипуляция

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.





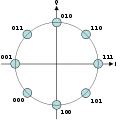
Двоичная фазовая манипуляция (BPSK)



Квадратурная фазовая манипуляция (QPSK)

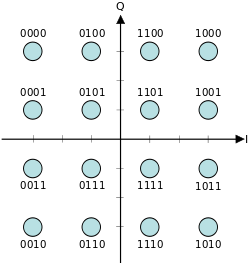
При **квадратурной фазовой манипуляции** (англ. *QPSK — Quadrature Phase Shift Keying* или 4-PSK) используется созвездие из четырёх точек, размещённых на равных расстояниях на окружности. Используя 4 фазы, в QPSK на символ приходится два бита, как показано на рисунке. Анализ показывает, что скорость 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)

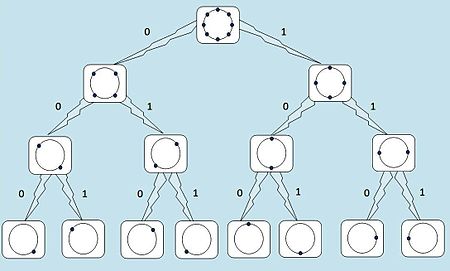
### Квадратурная амплитудная манипуляция



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

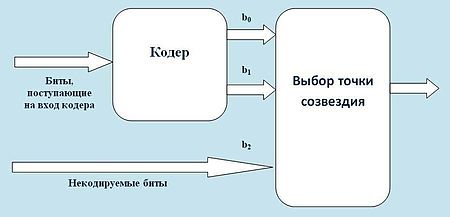
Квадратурная амплитудная манипуляция (КАМ, англ. Quadrature amplitude modulation (QAM)) — манипуляция, при которой изменяется как фаза, так и амплитуда сигнала, что позволяет увеличить количество информации, передаваемой одним состоянием (отсчётом) сигнала. В англоязычной литературе такой тип манипуляции 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 (TCM), которая впервые была разработана в 1982 году Унгербоком. В основе TCM лежит совместный процесс кодирования и манипуляции.

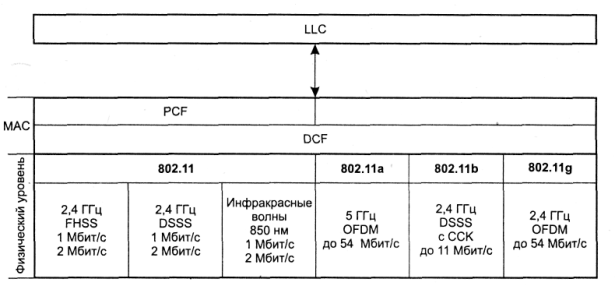


# Лекция 4. Стандарт 802.11 (WiFi). Уровень доступа к среде

* + - 1. **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](http://www.intuit.ru/department/network/wifi/2/#image.2.1%23image.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

* + - 1. **Уровень доступа к среде стандарта 802.11**

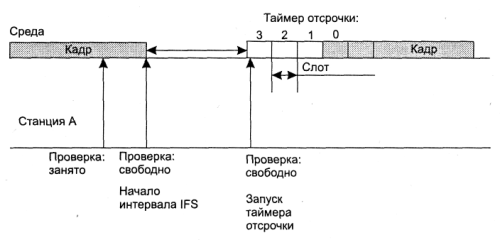
В сетях 802.11 уровень MAC обеспечивает два режима доступа к разделяемой среде (рис. 2.1):

* распределенный режим DCF (Distributed Coordination Function);
* централизованный режим PCF (Point Coordination Function).
  + - * 1. **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](http://www.intuit.ru/department/network/wifi/2/#image.2.2%23image.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 АСК 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](http://www.intuit.ru/department/network/wifi/2/1.html#image.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.

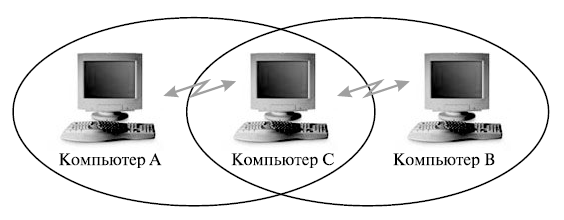
Размер слота зависит от способа кодирования сигнала; так, для метода FHSS размер слота равен 28 мкс, а для метода DSSS - 1 мкс. Размер слота выбирается таким образом, чтобы он превосходил время распространения сигнала между любыми двумя станциями сети плюс время, затрачиваемое станцией на распознавание 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 (А и В) удалены и не слышат друг друга, однако оба попадают в зону охвата третьего устройства С ([рис. 2.3](http://www.intuit.ru/department/network/wifi/2/2.html#image.2.3%23image.2.3)) - так называемая проблема скрытого терминала. Если оба устройства А и В начнут передачу, то они принципиально не смогут обнаружить конфликтную ситуацию и определить, почему пакеты не проходят.



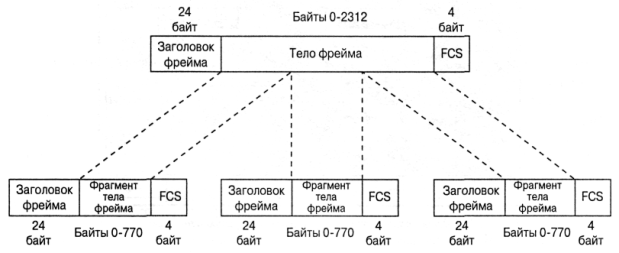
**Рис. 2.3.**  Проблема скрытого терминала

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](http://www.intuit.ru/department/network/wifi/2/2.html#image.2.4%23image.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

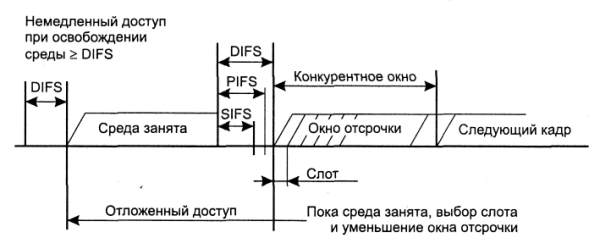
Размер фрагмента может задавать администратор сети. Фрагментации подвергаются только одноадресные фреймы. Широковещательные, или многоадресные, фреймы передаются целиком. Кроме того, фрагменты фрейма передаются пакетом, с использованием только одной итерации механизма доступа к среде DCF.

Хотя за счет фрагментации можно повысить надежность передачи фреймов в беспроводных локальных сетях, она приводит к увеличению "накладных расходов" МАС-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 МАС-протокола и снижает реальную производительность беспроводной станции. Фрагментация - это баланс между надежностью и непроизводительной загрузкой среды.

* + - * 1. **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](http://www.intuit.ru/department/network/wifi/2/3.html#image.2.5%23image.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.

* + - 1. **Кадр МАС-подуровня**

На [рис. 2.6](http://www.intuit.ru/department/network/wifi/2/3.html#image.2.6%23image.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.



**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](http://www.intuit.ru/department/network/wifi/2/3.html#image.2.7%23image.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](http://www.intuit.ru/department/network/wifi/2/3.html#table.2.1%23table.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-oпpoc |
| 01 | Контроль | 1011 | Запрос передачи |
| 01 | Контроль | 1100 | "Готов к передаче" |
| 01 | Контроль | 1101 | Подтверждение |
| 01 | Контроль | 1110 | Без состязания (СF)-конец |
| 01 | Контроль | 1111 | CF-конец + CF-подтверждение |
| 10 | Данные | 0000 | Данные |
| 10 | Данные | 0001 | Данные + CF-подтверждение |
| 10 | Данные | 0010 | Данные + CF-oпpoc |
| 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-oпрос |
| 10 | Данные | 0111 | Данные + CF-подтверждение + CF-oпрос |

* 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-onpoc). 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 (АСК). Подтверждение успешного приема предыдущих данных, кадра управления или кадра "PS-oпpoc".
* 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-onpoc. 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-onpoc. 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-oпpoc, CF-подтверждение + CF-oпpoc) имеют те же функции, что и описанные выше подтипы кадров (данные + CF-подтверждение, данные + CF-oпpoc, данные + CF-подтверждение + CF-oпpoc), 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 802.11а 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 МАС 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, 802.11а и 802.11g.

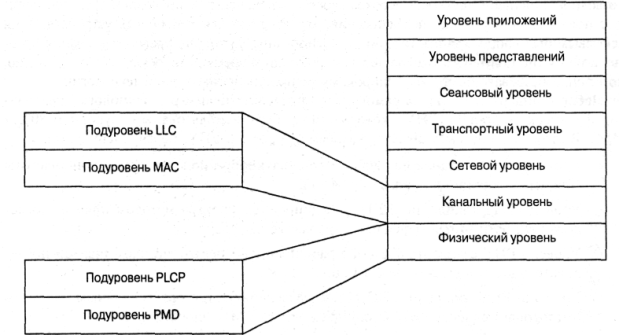
Каждый из физических уровней стандарта 802.11 имеет два подуровня:

* 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 МАС-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.

* + - 1. **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.
  + - * 1. **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.

* + - * 1. **Беспроводные локальные сети со скачкообразной перестройкой частоты (FHSS)**

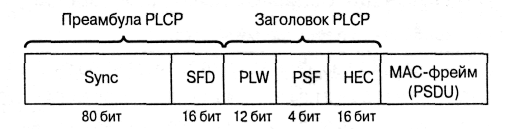
Беспроводные локальные сети FHSS поддерживают скорости передачи 1 и 2 Мбит/с. Устройства FHSS делят предназначенную для их работы полосу частот от 2,402 до 2,480 ГГц на 79 неперекрывающихся каналов (это справедливо для Северной Америки и большей части Европы). Ширина каждого из 79 каналов составляет 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](http://www.intuit.ru/department/network/wifi/3/2.html#table.3.1%23table.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 МАС-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

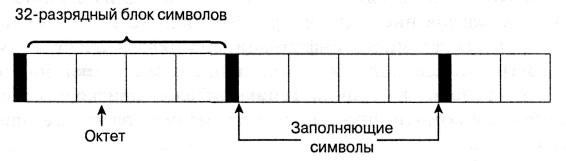
Преамбула PLCP состоит из двух подполей:

* 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](http://www.intuit.ru/department/network/wifi/3/2.html#image.3.3%23image.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.



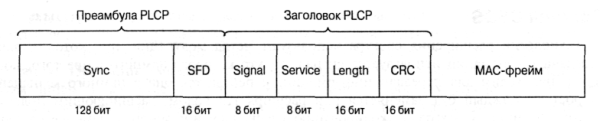
**Рис. 3.3.**  Скрэмблированный PSDU в технологии FHSS

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).

* + - * 1. **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](http://www.intuit.ru/department/network/wifi/3/2.html#image.3.4%23image.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 ОхF3A0; 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.

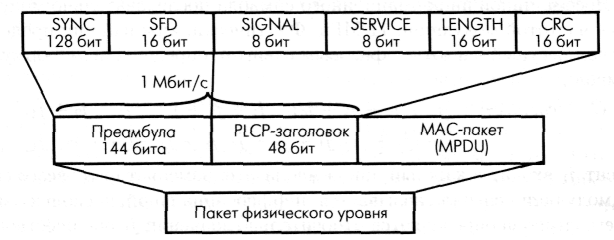
Подуровень PLCP преобразует фрейм в поток битов и передает данные на подуровень PMD. Весь PPDU проходит через процесс скрэмблирования с целью рандомизации данных.

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.
  + - 1. **IEEE 802.11b**

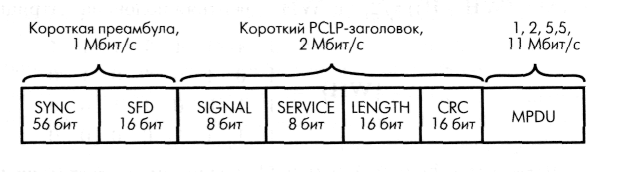
На физическом уровне к МАС-кадрам (MPDU) добавляется заголовок физического уровня, состоящий из преамбулы и собственно PLCP-заголовка ([рис. 3.5](http://www.intuit.ru/department/network/wifi/3/3.html#image.3.5%23image.3.5)).

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](http://www.intuit.ru/department/network/wifi/3/3.html#image.3.6%23image.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: В1 = (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 bЗ). Последние два бита (b2 и bЗ) используются для определения 8 последовательностей комплексных чипов, как показано в таблице 1.3, где {cl, с2, сЗ, с4, с5, с6, с7, с8} представляют чипы последовательности. В [таблице 3.2](http://www.intuit.ru/department/network/wifi/3/3.html#table.3.2%23table.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, bЗ) | С1 | С2 | С3 | С4 | С5 | С6 | С7 | С8 |
| 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, bЗ), 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](http://www.intuit.ru/department/network/wifi/3/3.html#table.3.3%23table.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 |  |
| 01 | /2 | -/2 |
| 11 |  | 0 |
| 10 | -/2 | /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, bЗ) 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.

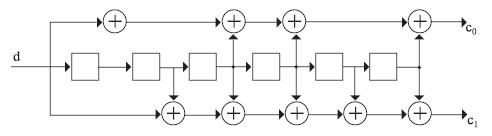
На практике важно не только операционное усиление. Существенную роль играет и равномерность распределения символов в фазовом пространстве - они должны как можно дальше отстоять друг от друга, чтобы минимизировать ошибки их детектирования. И с этой точки зрения ССК-модуляция не выглядит оптимальной, ее реальное операционное усиление не превышает 2 дБ. Поэтому изначально прорабатывался другой способ модуляции - пакетное бинарное сверточное кодирование РВСС (Packet Binary Convolutional Coding). Этот метод вошел в стандарт IEEE 802.11b как дополнительная (необязательная) опция. Механизм РВСС ([рис. 3.7](http://www.intuit.ru/department/network/wifi/3/3.html#image.3.7%23image.3.7)) позволяет добиваться в сетях IEEE 802.11b пропускной способности 5,5, 11 и 22 Мбит/с.



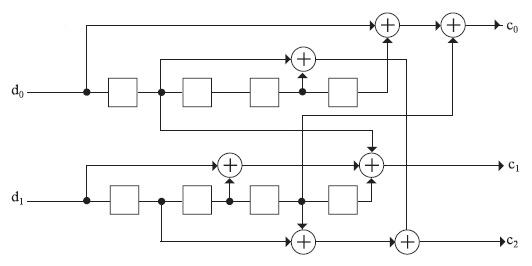
**Рис. 3.7.**  Общая схема РВСС-модуляции

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](http://www.intuit.ru/department/network/wifi/3/3.html#image.3.8%23image.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 с0 и c1 задают один символ четырехпозиционной QPSK-модуляции. Для скорости 5,5 Мбит/с используют двухпозиционную BPSK-модуляцию, последовательно передавая кодовые биты c0 и с1. Если же нужна скорость 22 Мбит/с, схема кодирования усложняется ([рис. 3.9](http://www.intuit.ru/department/network/wifi/3/3.html#image.3.9%23image.3.9)): три кодовых бита (c0-c2) определяют один символ в 8-позиционной 8-РSК-модуляции.

После формирования PSK-символов происходит скрэмблирование. В зависимости от сигнала s ([рис. 3.3](http://www.intuit.ru/department/network/wifi/3/2.html#image.3.3)) символ остается без изменений (s = 0), либо его фаза увеличивается на /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 РВСС для скоростей 11 и 5,5 Мбит/с, 64 возможных выходных состояния. Так что при модуляции РВСС информационные биты в фазовом пространстве оказываются гораздо дальше друг от друга, чем при ССК-модуляции. Поэтому РВСС и позволяет при одном и том же соотношении "сигнал-шум" и уровне ошибок вести передачу с большей скоростью, чем в случае СКК. Однако плата за более эффективное кодирование - сложность аппаратной реализации данного алгоритма.

* + - 1. **IEEE 802.11а**

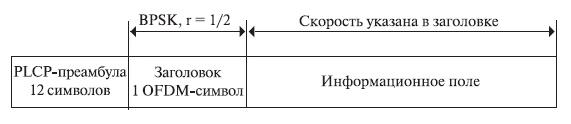
Стандарт IEEE 802.11а появился практически одновременно с IEEE 802.11b, в сентябре 1999 года. Эта спецификация была ориентирована на работу в диапазоне 5 ГГц и основана на принципиально ином, чем описано выше, механизме кодирования данных - на частотном мультиплексировании посредством ортогональных несущих (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 802.11а 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](http://www.intuit.ru/department/network/wifi/3/4.html#table.3.4%23table.3.4) показано, как необходимая скорость передачи данных преобразуется в соответствующие параметры узлов передатчика OFDM.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Таблица 3.4. Параметры передатчика стандарта 802.11а | | | | | |
| **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 |

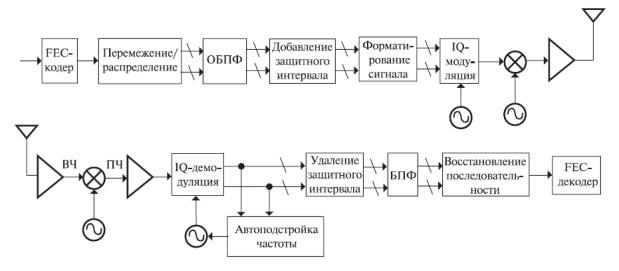
Из 52 несущих 48 предназначены для передачи информационных символов, остальные 4 - служебные. Структура заголовков физического уровня отличается от принятого в спецификации IEEE 802.11b, но незначительно ([рис. 3.10](http://www.intuit.ru/department/network/wifi/3/4.html#image.3.10%23image.3.10)).



**Рис. 3.10.**  Структура заголовка физического уровня стандарта IEEE 802.11а

Кадр включает преамбулу (12 символов синхропоследовательности), заголовок физического уровня (PLCP-заголовок) и собственно информационное поле, сформированное на МАС-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](http://www.intuit.ru/department/network/wifi/3/4.html#image.3.11%23image.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 802.11а

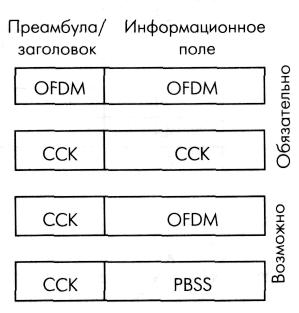
* + - 1. **IEEE 802.11g**

Стандарт IEEE 802.11g по сути представляет собой перенесение схемы модуляции OFDM, прекрасно зарекомендовавшей себя в 802.11а, 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 ССК (Complementary Code Keying), а в качестве дополнительной возможности допускается модуляция PBSS.

Разработчики 802.11g предусмотрели ССК-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](http://www.intuit.ru/department/network/wifi/3/5.html#image.3.12%23image.3.12)).

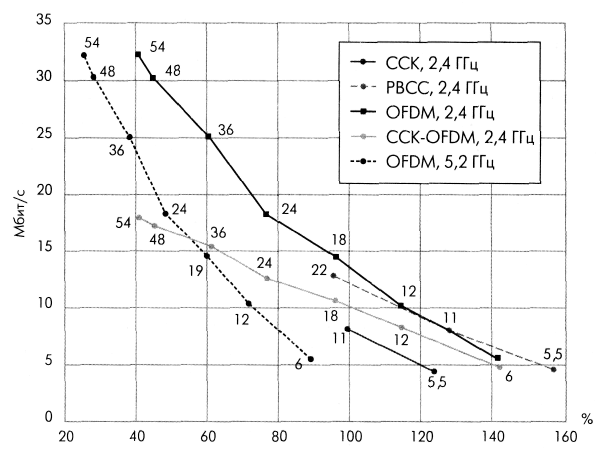


**Рис. 3.12.**  Кадры IEEE 802.11g в различных режимах модуляции

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 ССК (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 ССК, 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](http://www.intuit.ru/department/network/wifi/3/5.html#table.3.5%23table.3.5), зависимость скорости от типа модуляции - на [рис. 3.13](http://www.intuit.ru/department/network/wifi/3/5.html#image.3.13%23image.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 | РВСС |
| 6 | OFDM | OFDM |
| 9 |  | OFDM, CCK-OFDM |
| 11 | CCK | РВСС |
| 12 | OFDM | CCK-OFDM |
| 18 |  | OFDM, CCK-OFDM |
| 22 |  | РВСС |
| 24 | OFDM | CCK-OFDM |
| 33 |  | РВСС |
| 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.

* 1. ***Стандарт 802.11n***

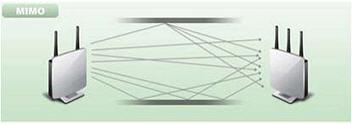
для сетей Wi-Fi был утвержден организацией IEEE (Институт инженеров по электротехнике и радиоэлектронике) 11 сентября 2009 года.

В основе стандарта 802.11n:

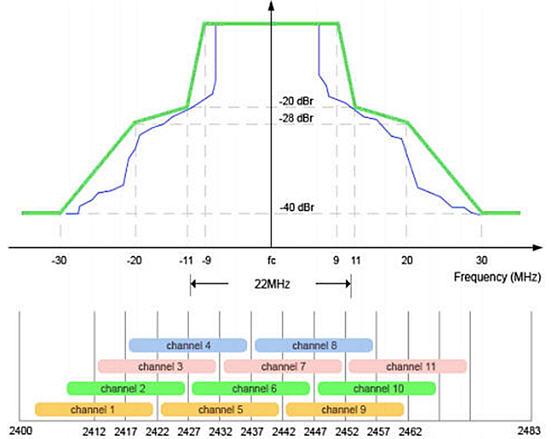
* *Увеличение скорости передачи данных;*
* *Увеличение зоны покрытия;*
* *Увеличение надежности передачи сигнала;*
* *Увеличение пропускной способности.*

**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.

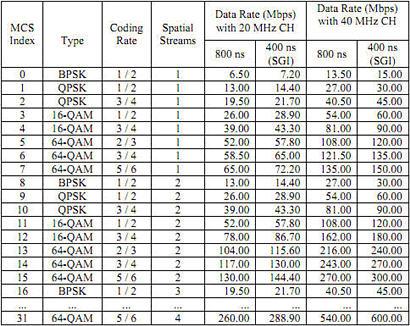


Чем больше устройство 802.11n использует антенн для одновременной работы передачи/приема, тем будет выше максимальная скорость передачи данных. Однако, само по себе использование нескольких антенн не увеличивает скорость передачи данных или расширение диапазона. Основным в устройствах стандарта 802.11n 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 c 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 "4х4").  
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:



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](http://www.intuit.ru/department/network/wifi/3/5.html#table.3.6%23table.3.6) представлена сводная информация по параметрам физических уровней.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Таблица 3.6. Стандарты физического уровня | | | | | |
| **Параметр** | **802.11 DSSS** | **802.11 FHSS** | **802.11b** | **802.11а** | **802.11g** |
| Частотный диапазон (ГГц) | 2,4 | 2,4 | 2,4 | 5 | 2,4 |
| Максимальная скорость передачи данных (Мбит/c) | 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**

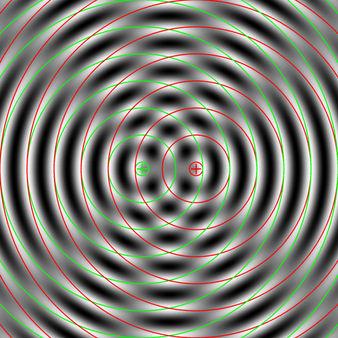
Принятие финальной версии спецификации 802.11ac состоялось в январе 2014 года

* 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**

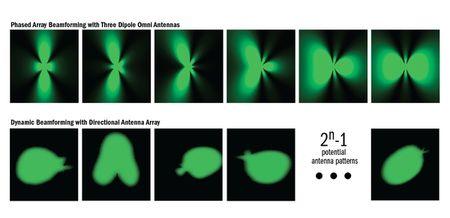
Как видно из предыдушей фотографии уровня помех, формирование лучей с всенаправленных антенн происходит в многочисленных, часто противоположных, направлениях. Изменяя синхронизацию сигналов на каждой антенне, можно контролировать форму модели формирования луча. Это неплохо, потому что позволяет сфокусировать 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**

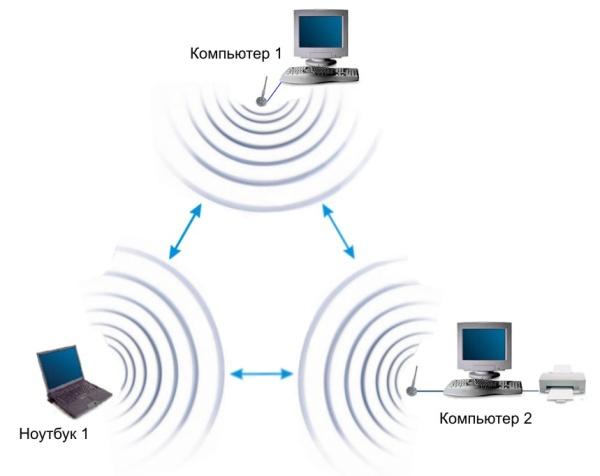
Беспроводные сети Wi-Fi поддерживают несколько различных режимов работы, реализуемых для конкретных целей. Каждый режим сопровождается пояснительным рисунком для лучшего представления взаимодействия элементов сети. Большим плюсом является подробное описание настройки подключения, используя как встроенные 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.

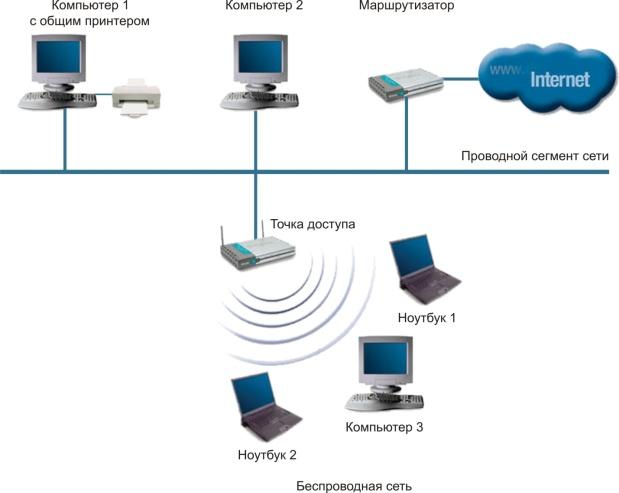
Основное достоинство данного режима - простота организации: он не требует дополнительного оборудования (точки доступа). Режим может применяться для создания временных сетей для передачи данных.

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.



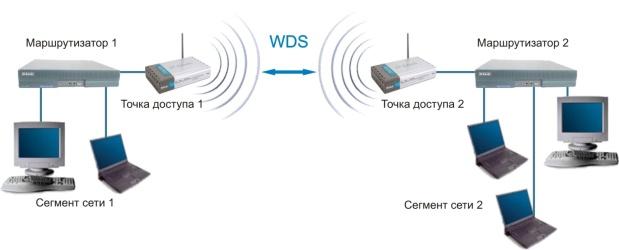
## Инфраструктурный режим

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.



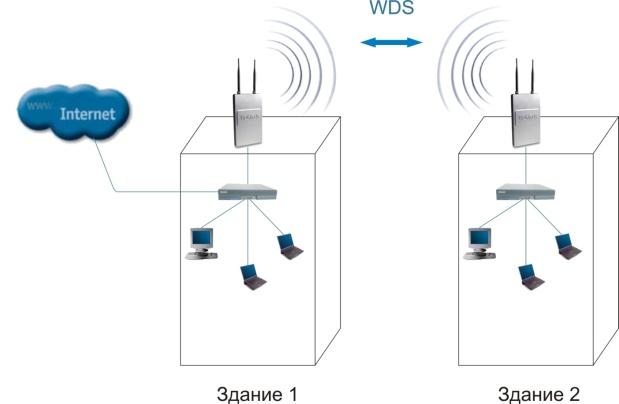
## Режимы WDS и WDS WITH AP

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.

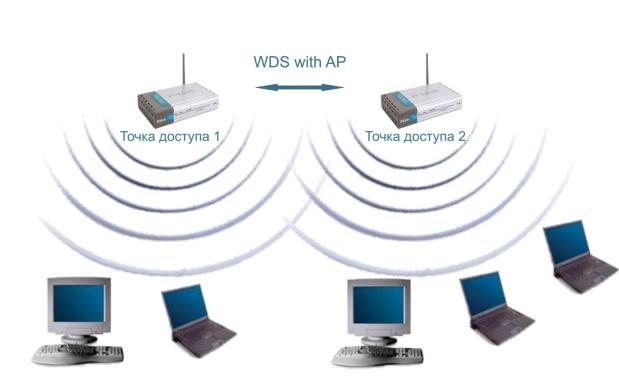


## Мостовой режим между зданиями

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 АР (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.



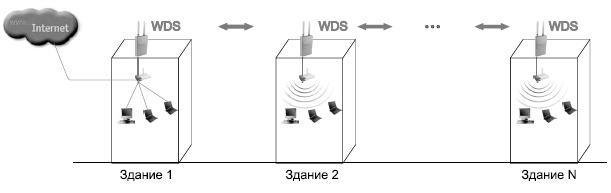
## Режим WDS with AP

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.

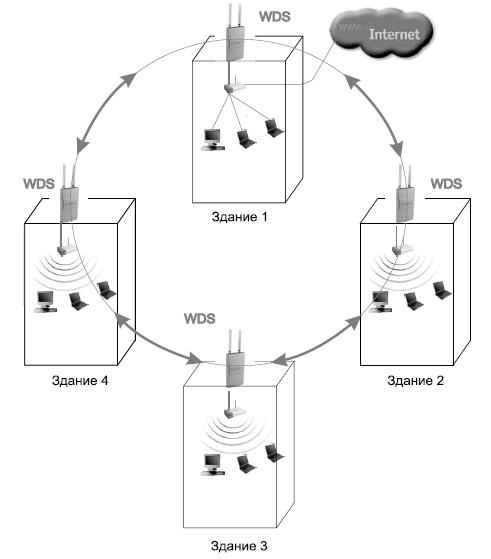
Шине не страшны отказы отдельных точек, так как все остальные компьютеры сети могут нормально продолжать обмен между собой, но при этом оставшаяся часть компьютеров не сможет получить доступ в Internet.

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.

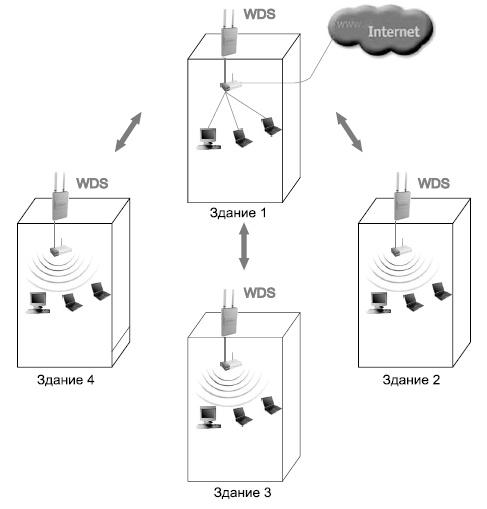
Топология связей между точками в этом режиме представляет собой ациклический граф типа "дерево", то есть данные из Internet от точки 4 к точке 2 проходят по двум направлениям - через точку 1 и 3 ( рис. 4.15). Для устранения лишних связей, способных приводить к появлению циклов в графе, реализуется алгоритм 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.



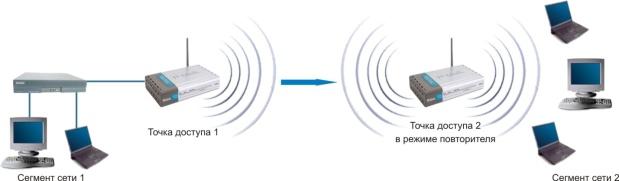
Топология типа "звезда"

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

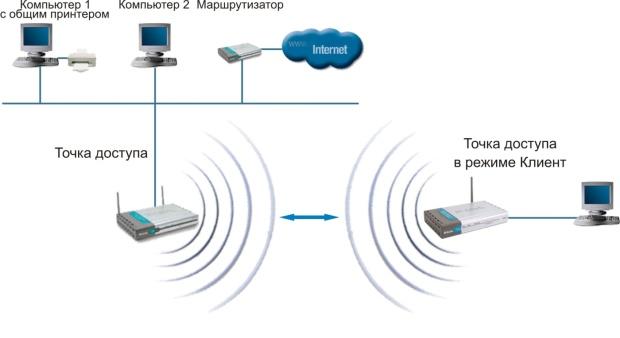
Аналогично проводному повторителю, беспроводной повторитель просто ретранслирует все пакеты, поступившие на его беспроводной интерфейс. Эта ретрансляция осуществляется через тот же канал, через который они были получены.

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 МАС-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.

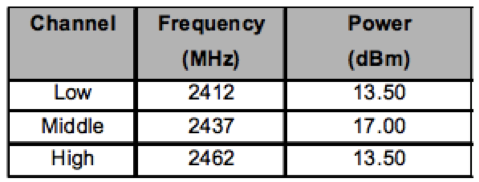
Самым близким аналогом Wi-Fi Direct являются старые специальные сети, ранний вариант Wi-Fi, который связывал 2 или более устройств без роутера.

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.

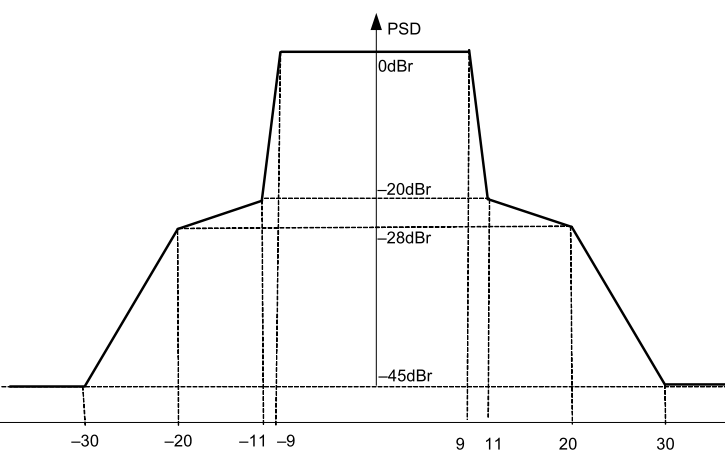
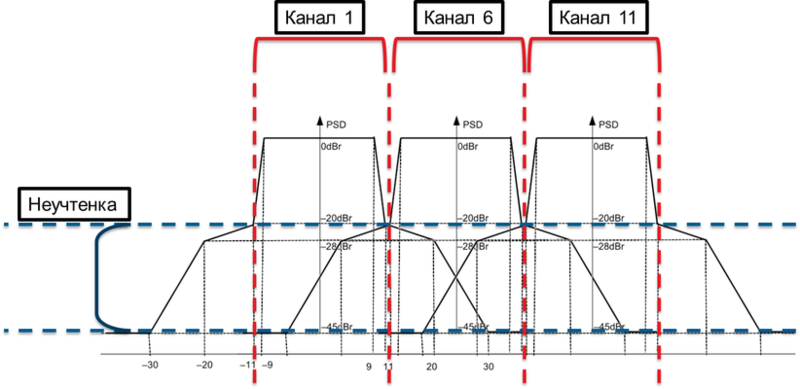
# Лекция 7. Особенности использования сетей WiFi

**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](https://apps.fcc.gov/eas/GetApplicationAttachment.html?id=1544473) (мощность на порту антенны).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!

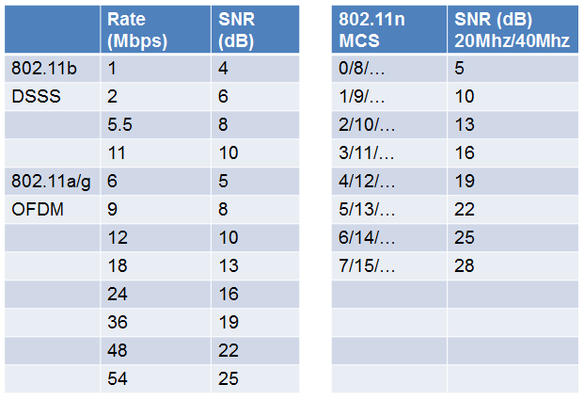
**Почему**

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].  
  
В сетях 802.11n/MIMO благодаря [MRC](http://en.wikipedia.org/wiki/Maximal-ratio_combining) и другим многоантенным ухищрениям нужный SNR можно получить и при более низком входном сигнале. Обычно, это отражено в значениях чувствительности в datasheet'ах.  
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](http://en.wikipedia.org/wiki/List_of_WLAN_channels#5.C2.A0GHz_.28802.11a.2Fh.2Fj.2Fn.29.5B13.5D)). В итоге, связь может периодически пропадать.

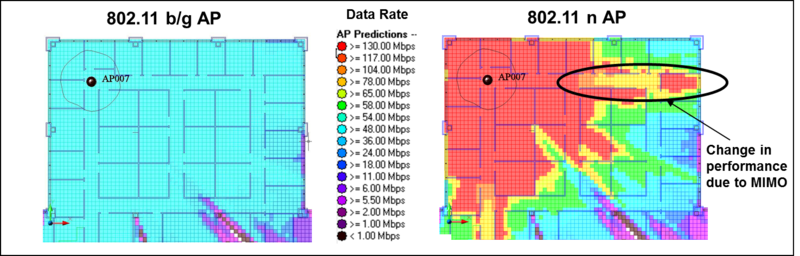
**4. Раз уж речь зашла о безопасности…**

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 асммметричную 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).

Cледует 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 A до точки B — 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]](https://ru.wikipedia.org/wiki/%D0%AF%D1%87%D0%B5%D0%B8%D1%81%D1%82%D0%B0%D1%8F_%D1%82%D0%BE%D0%BF%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D1%8F#cite_note-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. АР 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 МР, 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 МАС-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 МАС-уровня.

Структура пакетов MAC-уровня в mesh-сети аналогична стандартному формату пакетов сетей 802.11. Формат заголовка МАС-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.

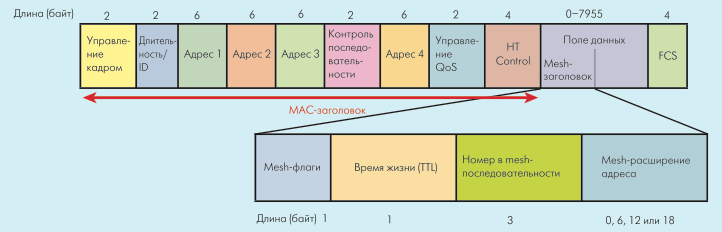
Отличие МАС-пакетов 802.11s заключается в наличии mesh-заголовка в начале поля данных. Этот заголовок присутствует в пакетах данных тогда и только тогда, когда они передаются от mesh-узла к mesh-узлу по установленному между ними соединению, он так же присоединяется к одному из типов (Multihop Action) 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 МАСуровня 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 МР. Это возможно, если узлы вне mesh-сети общаются через mesh-сеть. Возможен и случай, когда два МР-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 МР могут, но не обязаны поддерживать глобальную синхронизацию в сети. Соответственно, они подразделяются на синхронные и асинхронные МР. Асинхронные МР 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 МР стараются поддерживать общее для всех время Mesh TSF.

Синхронные МР передают биконы по тому же алгоритму, что и в сетях ad hoc, за исключением следующего аспекта. Если МР 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 МР 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 cетях 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 МР 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 ВВ выбран, оставшиеся МР биконы не передают. Роль ВВ периодически передается от одного МР другому. Однако в mesh-сети некоторые станции скрыты друг от друга, что приводит к появлению нескольких ВВ, и задача ротации ВВ становится слишком сложной. В связи с этим в более поздних версиях стандарта meshсетей использование ВВ 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 МР. Поэтому вместо поддержки глобальной синхронизации МР могут лишь поддерживать синхронизацию попарно. При этом МР 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 МР, 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 c 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 МР. Так, асинхронные МР используют свои собственные значения ATIM и DTIM, а все узлы, с которыми они установили соединение, сохраняют эти параметры для дальнейшей работы. Синхронные же МР, 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

# Лекция 10. Bluetooth.

**Bluetooth** (от слов англ. *blue* синий и англ. *tooth* зуб; произносится /bluːtuːθ/) — 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. В 2002 году Bluetooth был стандартизован в IEEE (Institute of Electrical and Electronics Engineers), как стандарт 802.15.1.

BluetoothLogo.svg

## Название и логотип

Слово Bluetooth — перевод на английский язык датского слова «Blåtand» («Синезубый»). Так прозвали когда-то короля викингов Харальда I Синезубого, жившего в Дании около тысячи лет назад. Прозвище это король получил за темный передний зуб. Харальд I правил в X веке Данией и частью Норвегии и объединил враждовавшие датские племена в единое королевство. Подразумевается, что Bluetooth делает то же самое с протоколами связи, объединяя их в один универсальный стандарт. Хотя «blå» в современных скандинавских языках означает «синий», во времена викингов оно также могло означать «чёрного цвета». Таким образом, исторически правильно было бы перевести датское *Harald Blåtand* скорее как *Harald Blacktooth*, чем как *Harald Bluetooth*.

Логотип Bluetooth является сочетанием двух нордических («скандинавских») рун: «хаглаз» H-rune.gif (Hagall) — аналог латинской H и «беркана» Runic letter berkanan.svg (Berkanan) — латинская B. Логотип похож на более старый логотип для Beauknit Textiles, подразделения корпорации Beauknit. В нём используется слияние отраженной K и В для «Beauknit», он шире и имеет скругленные углы, но в общем он такой же.

Принцип действия основан на использовании радиоволн. Радиосвязь Bluetooth осуществляется в ISM-диапазоне (англ. *Industry, Science and Medicine*), который используется в различных бытовых приборах и беспроводных сетях (свободный от лицензирования диапазон 2,4-2,4835 ГГц). В Bluetooth применяется метод расширения спектра со скачкообразной перестройкой частотs (англ. *Frequency Hopping Spread Spectrum, FHSS*). Метод FHSS прост в реализации, обеспечивает устойчивость к широкополосным помехам, а оборудование недорого.

Согласно алгоритму FHSS, в Bluetooth несущая частота сигнала скачкообразно меняется 1600 раз в секунду (всего выделяется 79 рабочих частот шириной в 1 МГц, а в Японии, Франции и Испании полоса у́же — 23 частотных канала). Последовательность переключения между частотами для каждого соединения является псевдослучайной и известна только передатчику и приёмнику, которые каждые 625 мкс (один временной слот) синхронно перестраиваются с одной несущей частоты на другую. Таким образом, если рядом работают несколько пар приёмник-передатчик, то они не мешают друг другу. Этот алгоритм является также составной частью системы защиты конфиденциальности передаваемой информации: переход происходит по псевдослучайному алгоритму и определяется отдельно для каждого соединения. При передаче цифровых данных и аудиосигнала (64 кбит/с в обоих направлениях) используются различные схемы кодирования: аудиосигнал не повторяется (как правило), а цифровые данные в случае утери пакета информации будут переданы повторно.

Протокол Bluetooth поддерживает не только соединение «point-to-point», но и соединение «point-to-multipoint».

### Bluetooth 1.0

Устройства версий 1.0 (1998) и 1.0B имели плохую совместимость между продуктами различных производителей. В 1.0 и 1.0B была обязательной передача адреса устройства (BD\_ADDR) на этапе установления связи, что делало невозможной реализацию анонимности соединения на протокольном уровне и было основным недостатком данной спецификации. Скорость 721 Кбит/с. Стандартная (базовая) скорость передачи данных использует GFSK-модуляцию радиосигнала при скорости передачи в 1 Мбит/с.

#### Bluetooth 1.1

В Bluetooth 1.1 было исправлено множество ошибок, найденных в 1.0B, добавлена поддержка для нешифрованных каналов, индикация уровня мощности принимаемого сигнала (RSSI).

#### Bluetooth 1.2

Главные улучшения включают следующее:

* Быстрое подключение и обнаружение.
* Адаптивная перестройка частоты с расширенным спектром (AFH), которая повышает стойкость к радиопомехам.
* Более высокие, чем в 1.1, скорости передачи данных, практически до 1 Мбит/с.
* Расширенные Синхронные Подключения (eSCO), которые улучшают качество передачи голоса в аудиопотоке, позволяя повторную передачу повреждённых пакетов, и при необходимости могут увеличить задержку аудио, чтобы оказать лучшую поддержку для параллельной передачи данных.
* В Host Controller Interface (HCI) добавлена поддержка трёхпроводного интерфейса UART.
* Утверждён как стандарт IEEE Standard 802.15.1-2005.
* Введены режимы управления потоком данных (Flow Control) и повторной передачи (Retransmission Modes) для L2CAP.

### Bluetooth 2.0 + EDR

Bluetooth версии 2.0 был выпущен 10 ноября 2004 г. Имеет обратную совместимость с предыдущими версиями 1.x. Основным нововведением стала поддержка Enhanced Data Rate (EDR) для ускорения передачи данных. Номинальная скорость EDR около 3 Мбит/с, однако на практике это позволило повысить скорость передачи данных только до 2,1 Мбит/с. Дополнительная производительность достигается с помощью различных радиотехнологий для передачи данных. EDR использует сочетание модуляций GFSK и PSK с двумя вариантами, π/4-DQPSK и 8DPSK. Они имеют большие скорости передачи данных по воздуху — 2 и 3 Mбит/с соответственно.

Bluetooth SIG издала спецификацию как «Технология Bluetooth 2.0 + EDR», которая подразумевает, что EDR является дополнительной функцией. Кроме EDR, есть и другие незначительные усовершенствования к 2.0 спецификации, и продукты могут соответствовать «Технологии Bluetooth 2.0», не поддерживая более высокую скорость передачи данных. Пъ

Согласно 2.0 + EDR спецификации, EDR обеспечивает следующие преимущества:

* Увеличение скорости передачи в 3 раза (2,1 Мбит/с) в некоторых случаях.
* Уменьшение сложности нескольких одновременных подключений из-за дополнительной полосы пропускания.
* Снижение потребления энергии благодаря уменьшению нагрузки.

#### Bluetooth 2.1

2007 год. Добавлена технология расширенного запроса характеристик устройства (для дополнительной фильтрации списка при сопряжении), энергосберегающая технология Sniff Subrating, которая позволяет увеличить продолжительность работы устройства от одного заряда аккумулятора в 3—10 раз. Кроме того обновлённая спецификация существенно упрощает и ускоряет установление связи между двумя устройствами, позволяет производить обновление ключа шифрования без разрыва соединения, а также делает указанные соединения более защищёнными, благодаря использованию технологии Near Field Communication.

#### Поддержка Multi-cast

В персональных сетях часто возникает необходимость передать одни и те же данные нескольким устройствам в одно и то же время. Bluetooth 1.х предусматривал многократную передачу этих данных по очереди, для каждого устройства. В один момент в отдельной Bluetooth-сети могло присутствовать только одно передающее и одно принимающее устройство. Это очень затрудняло работу в реальном времени с такими задачами, как совместное прослушивание одного и того же аудио на нескольких Bluetooth-наушниках, или как компьютерные игры с несколькими участниками, синхронизирующимися по Bluetooth. Кроме того, это просто замедляет работу, так как каждый раз надо заново устанавливать связь с очередным устройством, что занимает заметное время.

В Bluetooth 2.0 предусмотрена возможность одновременной отправки нескольким устройствам одних и тех же данных. Эта возможность называется "Multi-cast", она стала возможна благодаря устранению механизма быстрых смен частотных каналов.

#### Система QoS (quality of service)

При использовании интерфейса Bluetooth для связи с несколькими устройствами одновременно часто возникают нежелательные задержки. Их можно было бы избежать, если бы потоки данных были лучше организованы.

Спецификация Bluetooth 2.0 предусматривает специальный механизм QoS (quality of service), который обеспечивает взаимодействие устройств с минимальным количеством задержек. Устройства, поддерживающие QoS, коммуницируют между собой с целью согласовать свои потребности в немедленной передаче данных и возможности безболезненно справиться с задержкой связи. Таким образом, без повышения реальной скорости передачи данных, удаётся устранить эффект притормаживания, который так раздражает пользователей.

#### Распределённый контроль доступа к среде

Модель сети в ранних версиях Bluetooth очень проста. Сеть имеет одно главное и от одного до семи подчинённых устройств. Данные могут передаваться только между главным ("master") и подчинённым ("slave") устройствами. При этом, главное устройство контролирует доступ устройств к среде передачи данных. Если главное устройство по какой-то причине покинет сеть, то остальная сеть не сможет функционировать.

В Bluetooth 2.0 появился новый протокол, который предусматривает распределённый контроль за доступом к среде передачи данных, что избавляет сеть от зависимости от единственного устройства. Как только главное устройство покидает сеть, его функции передаются другому устройству.

Кроме того, в Bluetooth 2.0 максимальный размер сети увеличен с 8 до 256 устройств. В версиях 1.х для увеличения сети предусматривался довольно неудобный механизм объединения простых Bluetooth-сетей ("piconet") в одну большую сеть ("scatternet"). При этом, одно и то же устройство являлось главным в одной простой сети и подчинённым в другой. В версии 2.0 всё значительно проще от одного до 255 подчинённых устройств соединяются с одним главным.

#### Усиленное энергосбережение

Возросшая скорость передачи данных в Bluetooth 2.0 привела к росту потребляемой устройствами мощности. Однако, потребляемая мощность выросла не так сильно, как скорость, поэтому общий расход энергии на передачу одного и того же объёма данных заметно сократился. Для большинства задач имеет место более чем двукратный выигрыш в сбережении энергии.

Более умная организация работы с данными также повлияла на энергопотребление в сторону его сокращения. Так, например, использование одновременной передачи данных нескольким устройствам заметно экономнее, чем передача этих данных каждому устройству отдельно.

#### Bluetooth 2.1 + EDR

В августе 2008 года Bluetooth SIG представил версию 2.1+EDR. Новая редакция Bluetooth снижает потребление энергии в 5 раз, повышает уровень защиты данных и облегчает распознавание и соединение Bluetooth-устройств благодаря уменьшению количества шагов, за которые оно выполняется.

### Bluetooth 3.0 + HS

3.0+HS была принята Bluetooth SIG 21 апреля 2009 года. Она поддерживает теоретическую скорость передачи данных до 24 Мбит/с. Её основной особенностью является добавление AMP (Alternate MAC/PHY), дополнение к 802.11 как высокоскоростное сообщение. Для AMP были предусмотрены две технологии: 802.11 и UWB, но UWB отсутствует в спецификации.

Модули с поддержкой новой спецификации соединяют в себе две радиосистемы: первая обеспечивает передачу данных в 3 Мбит/с (стандартная для Bluetooth 2.0) и имеет низкое энергопотребление; вторая совместима со стандартом 802.11 и обеспечивает возможность передачи данных со скоростью до 24 Мбит/с (сравнима со скоростью сетей Wi-Fi). Выбор радиосистемы для передачи данных зависит от размера передаваемого файла. Небольшие файлы передаются по медленному каналу, а большие — по высокоскоростному. Bluetooth 3.0 использует более общий стандарт 802.11 (без суффикса), то есть не совместим с такими спецификациями Wi-Fi, как 802.11b/g или 802.11n.

### Bluetooth 4.0

Bluetooth SIG утвердил спецификацию Bluetooth 4.0 30 июня 2010 года. Bluetooth 4.0 включает в себя протоколы Классический Bluetooth, Высокоскоростной Bluetooth и Bluetooth с низким энергопотреблением. Высокоскоростной Bluetooth основан на Wi-Fi, а Классический Bluetooth состоит из протоколов предыдущих спецификаций Bluetooth.

Протокол Bluetooth с низким энергопотреблением предназначен, прежде всего, для миниатюрных электронных датчиков (использующихся в спортивной обуви, тренажёрах, миниатюрных сенсорах, размещаемых на теле пациентов и т. д.). Низкое энергопотребление достигается за счёт использования особого алгоритма работы. Передатчик включается только на время отправки данных, что обеспечивает возможность работы от одной батарейки типа CR2032 в течение нескольких лет. Стандарт предоставляет скорость передачи данных в 1 Мбит/с при размере пакета данных 8—27 байт. В новой версии два Bluetooth-устройства смогут устанавливать соединение менее чем за 5 миллисекунд и поддерживать его на расстоянии до 100 м. Для этого используется усовершенствованная коррекция ошибок, а необходимый уровень безопасности обеспечивает 128-битное AES-шифрование.

Датчики температуры, давления, влажности, скорости передвижения и т. д. на базе этого стандарта могут передавать информацию на различные устройства контроля: мобильные телефоны, КПК, ПК и т. п.

*— низкое потребление энергии;*

*— высокая скорость передачи данных, до 24 Мбит/сек;*

*— увеличенная дальность действия, свыше 100 метров;*

### Bluetooth 4.1

В конце 2013 года Bluetooth Special Interest Group (SIG) представила спецификацию Bluetooth 4.1. Одно из улучшений, реализованных в спецификации Bluetooth 4.1, касается совместной работы Bluetooth и мобильной связи четвёртого поколения LTE. Стандарт предусматривает защиту от взаимных помех путём автоматического координирования передачи пакетов данных.

The Bluetooth SIG announced formal adoption of the Bluetooth v4.1 specification on 4 December 2013. This specification is an incremental software update to Bluetooth Specification v4.0, and not a hardware update. The update incorporates Bluetooth Core Specification Addenda (CSA 1, 2, 3 & 4) and adds new features that improve consumer usability. These include increased co-existence support for LTE, bulk data exchange rates—and aid developer innovation by allowing devices to support multiple roles simultaneously.

New features of this specification include:

* Mobile Wireless Service Coexistence Signaling
* Train Nudging and Generalized Interlaced Scanning
* Low Duty Cycle Directed Advertising
* L2CAP Connection Oriented and Dedicated Channels with Credit Based Flow Control
* Dual Mode and Topology
* LE Link Layer Topology
* 802.11n PAL
* Audio Architecture Updates for Wide Band Speech
* Fast Data Advertising Interval
* Limited Discovery Time[[74]](https://en.wikipedia.org/wiki/Bluetooth#cite_note-74)

Notice that some features were already available in a Core Specification Addendum (CSA) before the release of v4.1.

### Bluetooth v4.2

Bluetooth v4.2 was released on December 2, 2014. It Introduces some key features for [IoT](https://en.wikipedia.org/wiki/Internet_of_Things). Some features, such as Data Length Extension, require a hardware update. But some older Bluetooth hardware may receive some Bluetooth v4.2 features, such as privacy updates via firmware.

The major areas of improvement are:

* LE Data Packet Length Extension
* LE Secure Connections
* Link Layer Privacy
* Link Layer Extended Scanner Filter Policies
* IP connectivity for Bluetooth Smart devices to become available soon after the introduction of BT v4.2 via the new Internet Protocol Support Profile (IPSP).
* IPSP adds an IPv6 connection option for Bluetooth Smart, to support connected home and other [IoT](https://en.wikipedia.org/wiki/Internet_of_Things) implementations.

### Bluetooth 5.0

16-17 июня 2016 года Bluetooth Special Interest Group (SIG) представила спецификацию Bluetooth 5.0. Изменения коснулись в основном режима с низким потреблением и высокоскоростного режима.

В режиме Low Energy (LE) пропускная способность по сравнению с Bluetooth 4.2 будет увеличена в два раза. Эффективная дальность возрастёт в четыре раза.

В высокоскоростном режиме, на этот раз основанным на более быстром стандарте Wi-Fi, скорость будет увеличена в два-три раза.

В классическом режиме сохранится совместимость с предыдущими спецификациями Bluetooth. Но при этом увеличится энергоэффективность модулей.

Так же обещается увеличение в восемь раз количества одновременных подключений к одному модулю.

**Принцип работы**

Каждое устройство ВТ имеет радиопередатчик и приемник, работающие в диапазоне частот 2,4 ГГц. Этот диапазон в большинстве стран отведен для промышленной, научной и медицинской аппаратуры и не требует лицензирования, что обеспечивает повсеместную применимость устройств. Для ВТ используются радиоканалы с дискретной (двоичной) частотной модуляцией, несущая частота каналов F = 2402 + k (МГц) , где k 0,...,78, возможен сокращенный вариант с F = 2454 + k (k = 0,...,22) . Кодирование простое логической единице соответствует положительная девиация частоты, нулю отрицательная.

Передатчики могут быть трех классов мощности, с максимальной мощностью 1, 2,5 и 100. МВт, причем должна быть возможность понижения мощности с целью экономии энергии. Передача ведется с перескоком несущей частоты с одного радиоканала на другой, что помогает в борьбе с интерференцией и замираниями сигнала. Физический канал связи представляется определенной псевдослучайной последовательностью используемых радиоканалов (79 или 23 возможных частот).

Группа устройств, разделяющих один канал (то есть знающих одну и ту же последовательность перескоков), образует так называемую пикосеть (piconet) , в которую может входить от 2 до 8 устройств.

В каждой, пикосети имеется одно ведущее устройство и до 7 активных ведомых. Кроме того, в зоне охвата ведущего устройства в его же пикосети могут находиться "припаркованные" ведомые устройства: они тоже "знают" последовательность перескоков и синхронизируются (по перескокам) с мастером, но не могут обмениваться данными до тех пор, пока мастер не разрешит им активность. Каждое активное ведомое устройство пикосети имеет свой временный номер (1-7); когда ведомое устройство деактивируется (паркуется), оно отдает свой номер другим. При последующей активации оно уже может получить иной .

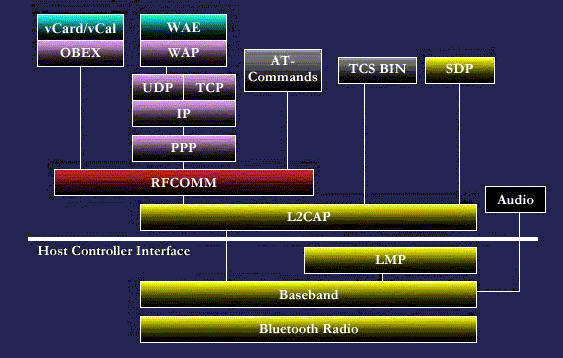
Между мастером и ведомыми устройствами могут устанавливаться физические связи двух типов: синхронные и асинхронные.

Синхронные связи (они же изохронные) с установлением соединения, SCO link (Synchronous Connection-Oriented) , используются для передачи изохронного графика (например, оцифрованного звука). Эти связи типа "точка-точка" предварительно устанавливаются мастером с выбранными ведомыми устройствами, и для каждой связи определяется период (в слотах), через который для нее резервируются слоты. Связи получаются симметричные двусторонние. Повторных передач пакетов в случае ошибок приема нет. Мастер может установить до трех связей SCO с одним или разными ведомыми устройствами. Ведомое устройство может иметь до трех связей с одним мастером или иметь по одной связи SCO с двумя различными мастерами. По сетевой классификации связи SCO относятся к коммутации цепей.

Асинхронные связи без установления соединения, ACL link (Asynchronous Connection-Less) , реализуют коммутацию пакетов по схеме "точка-множество точек" между мастером и всеми ведомыми устройствами пикосети. Мастер может связываться с любым из ведомых устройств пикосети в слотах, не занятых под SCO, послав ему пакет и потребовав ответа.

Ведомое устройство имеет право на передачу, только получив обращенный к нему запрос мастера (безошибочно декодировав свой адрес). Для большинства типов пакетов предусматривается повторная передача в случае обнаружения ошибки приема. Мастер может посылать и безадресные широковещательные пакеты для всех ведомых устройств своей пикосети. С каждым из своих ведомых устройств мастер может установить лишь одну связь ACL.

## Стек протоколов Bluetooth





Bluetooth имеет многоуровневую архитектуру, состоящую из основного протокола, протоколов замены кабеля, протоколов управления телефонией и заимствованных протоколов. Обязательными протоколами для всех стеков Bluetooth являются: LMP, L2CAP и SDP. Кроме того, устройства, связывающиеся с Bluetooth обычно используют протоколы HCI и RFCOMM.

**LMP**

Link Management Protocol — используется для установления и управления радиосоединением между двумя устройствами. Реализуется контроллером Bluetooth.

**L2CAP**

Logical Link Control and Adaptation Protocol — используется для мультиплексирования локальных соединений между двумя устройствами, использующими различные протоколы более высокого уровня. Позволяет фрагментировать и пересобирать пакеты.

**SDP**

Service Discovery Protocol — позволяет обнаруживать услуги, предоставляемые другими устройствами, и определять их параметры.

**RFCOMM**

Radio Frequency Communications — протокол замены кабеля, создаёт виртуальный последовательный поток данных и эмулирует управляющие сигналы RS-232.

**TCS**

Telephony Control Protocol – Binary — протокол, определяющий сигналы управления вызовом для установления голосовых соединений и соединений для передачи данных между устройствами Bluetooth. Используется только в профиле Cordless Telephony.

Заимствованные протоколы включают в себя: Point-to-Point Protocol (PPP), TCP/IP, UDP, Object Exchange Protocol (OBEX), Wireless Application Environment (WAE), Wireless Application Protocol (WAP).

## Профили Bluetooth

Профиль — набор функций или возможностей, доступных для определённого устройства Bluetooth. Для совместной работы Bluetooth-устройств необходимо, чтобы все они поддерживали общий профиль.

Нижеуказанные профили определены и одобрены группой разработки Bluetooth SIG:

* **Advanced Audio Distribution Profile** (A2DP) — разработан для передачи двухканального стерео аудиопотока, например, музыки, к беспроводной гарнитуре или любому другому устройству. Профиль полностью поддерживает низкокомпрессированный кодек Sub\_Band\_Codec (SBC) и опционально поддерживает MPEG-1,2 аудио, MPEG-2,4 AAC и ATRAC, способен поддерживать кодеки, определённые производителем.[[15]](https://ru.wikipedia.org/wiki/Bluetooth#cite_note-15)
* **Audio / Video Remote Control Profile** (AVRCP) — разработан для управления стандартными функциями телевизоров, Hi-Fi оборудования и прочего. То есть позволяет создавать устройства с функциями дистанционного управления. Может использоваться в связке с профилями A2DP или VDPT.
* **Basic Printing Profile** (BPP) — позволяет пересылать текст, сообщения электронной почты, vCard и другие элементы на принтер. Профиль не требует от принтера специфических драйверов, что выгодно отличает его от HCRP.
* **Dial-up Networking Profile** (DUN) — протокол предоставляет стандартный доступ к Интернету или другому телефонному сервису через Bluetooth. Базируется на SPP, включает в себя команды PPP и AT, определённые в спецификации ETSI 07.07.
* **Fax Profile** (FAX) — предоставляет интерфейс между мобильным или стационарным телефоном и ПК на котором установлено программное обеспечение для факсов. Поддерживает набор AT-команд в стиле ITU T.31 и/или ITU T.32. Голосовой звонок или передача данных профилем не поддерживается.
* **Human Interface Device Profile** (HID) — обеспечивает поддержку устройств с HID (Human Interface Device), таких как мышки, джойстики, клавиатуры и проч. Использует медленный канал, работает на пониженной мощности.
* **Headset Profile** (HSP) — используется для соединения беспроводной гарнитуры (Headset) и телефона. Поддерживает минимальный набор AT-команд спецификации GSM 07.07 для обеспечения возможности совершать звонки, отвечать на звонки, завершать звонок, настраивать громкость. Через профиль Headset, при наличии Bluetooth 1.2 и выше, можно выводить на гарнитуру всё звуковое сопровождение работы телефона. Например, прослушивать на гарнитуре все сигналы подтверждения операций, mp3-музыку из плеера, мелодии звонка, звуковой ряд видеороликов. Гарнитуры, поддерживающие такой профиль имеют возможность передачи стереозвука, в отличие от моделей, которые поддерживают только профиль Hands-Free.
* ***LAN Access Profile* (LAP)** — обеспечивает доступ Bluetooth-устройствам к вычислительным сетям LAN, WAN или Интернет посредством другого Bluetooth-устройства, которое имеет физическое подключение к этим сетям. Bluetooth-устройство использует PPP поверх RFCOMM для установки соединения. LAP также допускает создание ad-hoc Bluetooth-сетей.
* **Personal Area Networking Profile** (PAN) — позволяет использовать протокол Bluetooth Network Encapsulation в качестве транспорта через Bluetooth-соединение.
* ***Serial Port Profile*** (SPP) — базируется на спецификации ETSI TS07.10 и использует протокол RFCOMM. Профиль эмулирует последовательный порт, предоставляя возможность замены стандартного RS-232 беспроводным соединением. Является базовым для профилей DUN, FAX, HSP и AVRCP.
* **Synchronisation Profile** (SYNCH) — позволяет синхронизировать персональные данные (PIM). Профиль заимствован из спецификации инфракрасной связи и адаптирован группой Bluetooth SIG.

### Защита Bluetooth

Для защиты Bluetooth-соединения предусмотрено шифрование передаваемых данных, а также выполнение процедуры авторизации устройств. Шифрование данных происходит с ключом, эффективная длина которого — от 8 до 128 бит, что позволяет устанавливать уровень стойкости результирующего шифрования в соответствии с законодательством каждой страны. Поэтому стоит сразу отметить, что правильно сконфигурированные Bluetooth-устройства спонтанно соединяться не могут, поэтому случайных утечек важной информации к посторонним лицам не бывает. К тому же ничто не ограничивает защиту на уровне конкретных приложений.

В зависимости от выполняемых задач спецификация Bluetooth предусматривает три режима защиты, которые могут использоваться как по отдельности, так и в различных комбинациях:

1. В первом режиме — минимальном (который обычно применяется по умолчанию) — никаких мер для безопасного использования Bluetooth-устройства не предпринимается. Данные кодируются общим ключом и могут приниматься любыми устройствами без ограничений.
2. Во втором режиме осуществляется защита на уровне устройств, то есть активируются меры безопасности, основанные на процессах опознания/аутентификации (authentication) и разрешения/авторизации (authorization). В этом режиме определяются различные уровни доверия (trust) для каждой услуги, предложенной устройством. Уровень доступа может указываться непосредственно в чипе, и в соответствии с этим устройство будет получать определенные данные от других устройств.
3. Третий режим — защита на уровне сеанса связи, где данные кодируются 128-битными случайными числами, хранящимися в каждой паре устройств, участвующих в конкретном сеансе связи. Этот режим требует опознания и использует кодировку/шифрование данных (encryption).

Второй и третий режимы часто применяются одновременно. Главная задача процесса аутентификации состоит в том, чтобы проверить, действительно ли устройство, инициирующее сеанс связи, является именно тем, за которое себя выдает. Устройство, инициирующее связь, посылает свой адрес-идентификатор (Bluetooth Device Address, BD\_ADDR). Инициируемое устройство посылает в ответ случайное число в качестве запроса. В это время оба устройства рассчитывают опознавательный ответ, комбинируя адрес-идентификатор с полученным случайным числом. В результате сравнения происходит либо продолжение установления связи, либо разъединение (если опознавательные ответы не совпадут).

Если кто-то подслушивает соединение по эфиру, то для того, чтобы украсть аутентификационный ключ, ему необходимо знать алгоритм для выявления ключа из запроса и ответа, а определение такого обратного алгоритма потребует значительной компьютерной мощности. Поэтому стоимость извлечения ключа простым подслушиванием процедуры аутентификации неоправданно высока.

Что касается авторизации, то она предназначена для того, чтобы опознанное Bluetooth-устройство разрешило доступ к определенной информации или к услугам.

Существуют три уровня доверия между Bluetooth-устройствами: проверенное (trusted), не вызывающее доверия (non-trusted) и неизвестное (unknown). Если устройство имеет доверительные отношения с инициирующим, то последнему разрешается неограниченный доступ к ресурсам. Если же устройству не доверяют, то доступ к ресурсам ограничивается так называемыми защитными слоями обслуживания (layer security service). Например, первый защитный слой требует опознания и разрешения для открытия доступа к сервису, второй — только опознания, третий — только кодировки. Неизвестное устройство, которое не было опознано, считается непроверенным.

И наконец, 128-битное шифрование данных помогает защитить секретную информацию от просмотра нежелательными посетителями. Только адресат с личным расшифровывающим ключом (decryption key) имеет доступ к этим данным.

Расшифровывающий ключ устройства основан на ключе связи. Это упрощает процесс генерации ключа, так как отправитель и адресат обладают общей секретной информацией, которая расшифрует код.

Служба Bluetooth-шифрования имеет, в свою очередь, три режима:

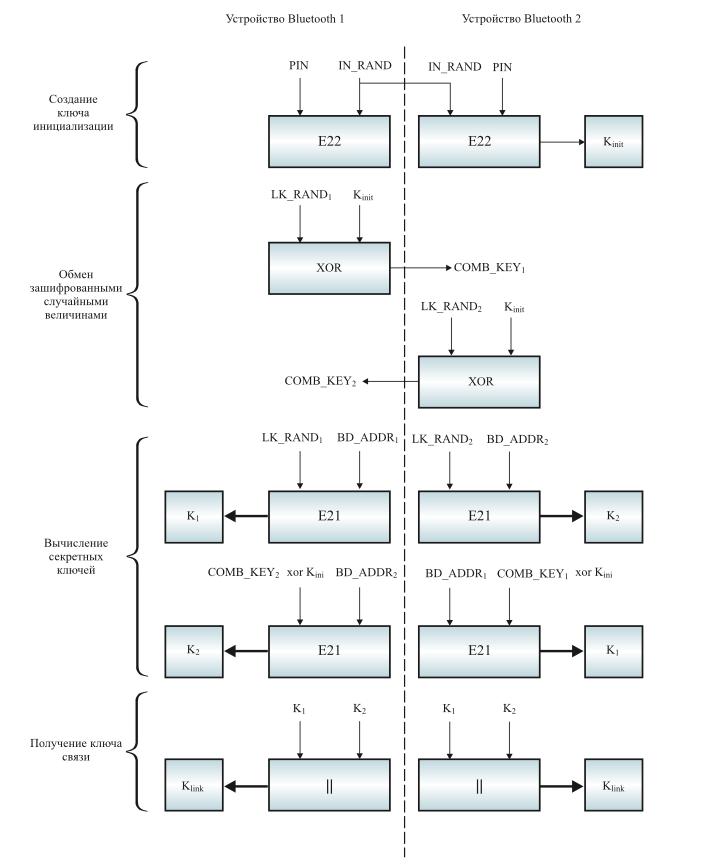
• режим без кодирования;

• режим, где кодируется только установление связи с устройствами, а передаваемая информация не кодируется;

• режим, при котором кодируются все виды связи.

Взаимодействие двух устройств по Bluetooth начинается с процедуры сопряжения (Pairing), при котором одно из устройств является главным (Master), а другое – ведомым (Slave). Пользователи, желающие осуществить передачу данных, вводят на своих устройствах PIN-код, который представляет собой любую UTF-8 строку длиной 16 байт. PIN-код вместе с адресом ведомого Bluetooth-устройства и 128-битным случайным числом (IN\_RAND) используется алгоритмом E22 для создания 128-битного ключа инициализации (Kinit), который затем будет применен при создании ключа связи.

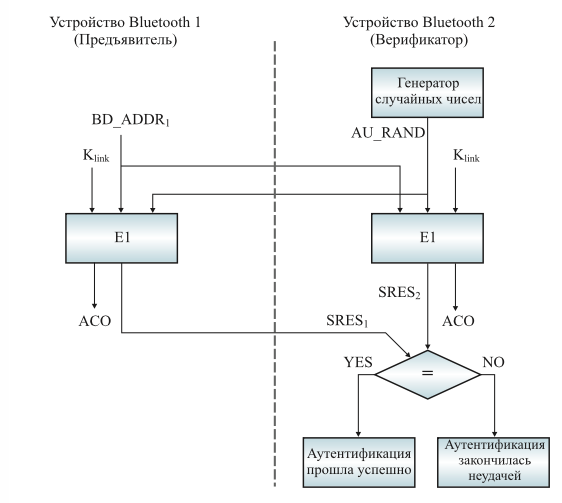
Для того чтобы создать разделяемый ключ, каждое из устройств генерирует случайное 128-битное число (LK\_RAND), которое затем вместе с адресом устройства шифруется алгоритмом E21 на ключе Kinit (побитовый XOR) и полученный COMB\_KEY отправляется другому устройству. Так как каждому из взаимодействующих устройств известен свой COMB\_KEY (ключ инициализации и адрес второго устройства), то каждое из устройств может легко получить COMB\_KEY второго устройства. Ключ связи (Klink) получается конкатенацией секретных ключей K1 и K2 обоих устройств.



После процедуры сопряжения следует процесс аутентификации. При этом одно из устройств является предъявителем, а второе верификатором. Предъявитель – это устройство, которое пытается подтвердить свою подлинность, верификатор – устройство, проверяющее подлинность. Возможен также сценарий взаимной проверки, при котором после прохождения аутентификации одним из устройств происходит смена ролей. Проверка подлинности базиру-

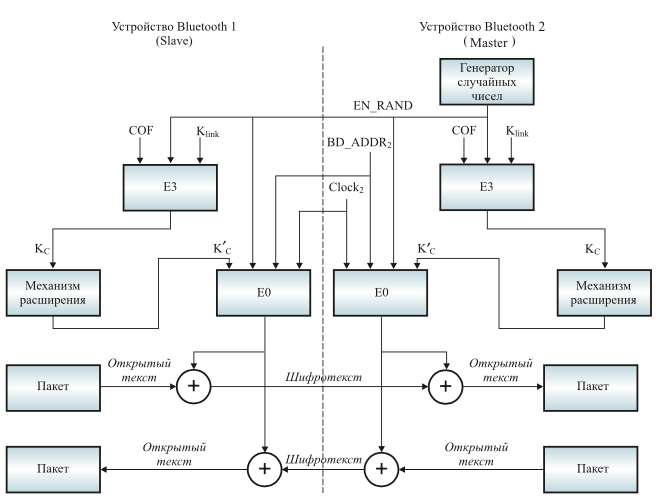
ется на проверке знания секретного ключа связи (Klink).

В случае успешного завершения процесса аутентификации, начинается процесс шифрования, если процесс аутентификации закончился неудачей, Bluetooth-устройство ждет некоторый промежуток времени, прежде чем повторить попытку. Этот временной интервал экспоненциально увеличивается, чтобы предотвратить попытку перебора ключа связи.



Основу процедуры шифрования Bluetooth составляет потоковый шифр E0, который для генерации гаммапоследовательности использует регистры сдвига с линейной обратной связью. Выходная гамма-последовательность накладывается на открытый текст с помощью операции XOR, после чего результат отправляется принимающему устройству. Дешифрование полностью симметрично. Шифруются только содержимое Bluetooth-пакетов; заголовки не шифруются никогда.

Для создания ключа шифрования (Kc) используется алгоритм E3, входными данными которого являются ключ связи (Klink), 128-битное случайное число (EN\_RAND), которое посылается от Master к Slave в открытом виде, и 96-бит COF (Ciphering Offset Number), основанный на ACO, получившимся в результате процесса аутентификации. Длина ключа шифрования варьируется от 8 до 128 бит (но всегда кратна 8 битам). Каждое устройство может работать с несколькими разными длинами Kc, поэтому устройства проходят фазу согласования, при которой выбирается максимальная длина ключа, поддерживаемая обоими устройствами. В качестве входных данных алгоритм E0 использует Bluetooth адрес Master-устройства, 26 бит системного времени Master-устройства и ключ шифрования Kc. В случае когда выбранная устройствами длина ключа шифрования меньше 128 бит, ключ будет уменьшен (Кc → Kc`) до установленного значения. [4]



Процесс шифрования представлен в общем виде на рисунке.

В основе алгоритмов E1, E2, E3 лежит симметричный блочный шифр SAFER+, который имеет уязвимости к некоторым видам атак, однако на сегодняшний момент обладает высоким запасом криптостойкости. Поточный шифр E0 имеет уязвимость к корреляционным атакам, о которой было известно разработчикам алгоритма, однако из-за высокой частоты ресинхронизации угроза была признана малозначимой. Долгое время атака оставалась чисто теоретической, однако в настоящее время наиболее эффективная из предложенных корреляционных атак позволяет получить ключ шифрования за 238 операций; если же известны первые 24 бита – 224 фреймов. Учитывая максимальное количество фреймов – 226, можно заключить, что данная атака может быть применена на практике.

Возможность проведения корреляционной атаки связана с наличием двух упущений в алгоритме E0. Первое из них связано с наличием смещения в конечном автомате (FSM), имеющем четыре бита состояния, один из которых комбинируется с выходами четырех регистров сдвига с линейной обратной связью (linear feedback shift register – LFSR) с помощью операции XOR, формируя выходной бит гаммапоследовательности. При удачном выборе комбинирующей функции вероятность того, что данный бит равен 1 (или соответственно 0) близка к 50%. Однако в FSM существует смещение:

*Pr (ct XOR ct+1 XOR ct+2 XOR ct+3 XOR ct+4 = 1) = 1/2 + 25/256*,

где *ct* – выходной бит FSM в момент времени *t*.

Таким образом, если ключ шифрования подобран верно, то гамма-последовательность будет иметь описанное выше смещение, в противном случае – не будет.

Второй недостаток алгоритма в том, что после загрузки входных значений (Klink, 128-битное случайное число, 48-битный адрес Master устройства, 26 бит системных часов Master устройства) в регистры LFSR, происходит генерация последовательности длиной 200 бит, последние 128 из которых перегружаются обратно в LFSR. При этом никаких преобразований не происходит за исключением изменения последовательности байт. Следовательно, легко отследить связь битов LFSR, использующихся для формирования выходного бита гамма-последовательности, с входными данными алгоритма.

Помимо недостаточновысокой криптостойкости использующегося для шифрования алгоритма, существует также недостаток в процедуре сопряжения. Безопасность протокола основана на секретности PIN-кода, длина которого должна составлять 16 байт, однако на практике, как правило, его длина составляет 4 или 6 десятичных символов (зачастую цифры), что позволяет, перехватив все использующиеся в процессе сопряжения данные, подобрать PIN-код методом полного перебора за секунды. В случае если злоумышленнику удастся пройти процедуру сопряжения, он получит доступ к весьма широкому спектру API-функций, что, по сути, означает контроль над устройством жертвы.

Итак, защитные функции Bluetooth должны обеспечивать безопасную коммуникацию на всех связующих уровнях. Но на практике, несмотря на предусмотренную стандартом безопасность, в этой технологии имеется целый ряд существенных изъянов.

Например, слабым местом защиты Bluetooth-устройств является то, что производители стремятся предоставить пользователям широкие полномочия и контроль над устройствами и их конфигурацией. В то же время современная Bluetooth-технология обладает недостаточными средствами для опознания пользователей (то есть система безопасности Bluetooth не принимает во внимание личность или намерения пользователя), что делает Bluetooth-устройства особенно уязвимыми к так называемым spoofing-нападениям (радиодезинформации) и неправильному применению опознавательных устройств.

Кроме того, приоритетным считается надежность опознавания устройств, а не их безопасное обслуживание. Поэтому обнаружение услуг (service discovery) является критической частью всей схемы Bluetooth.

Крайне слабым местом интерфейса Bluetooth можно считать и процесс первичного спаривания устройств (pairing), при котором происходит обмен ключами в незакодированных каналах, что делает их уязвимыми для стороннего прослушивания. В результате перехвата передачи в момент процесса спаривания можно получить ключ инициализации путем вычисления этих ключей для любого возможного варианта пароля и последующего сравнения результатов с перехваченной передачей. Ключ инициализации, в свою очередь, используется хакером для расчета ключа связи и сравнивается с перехваченной передачей для проверки. В связи с этим рекомендуется производить процедуру спаривания в знакомой и безопасной среде, что значительно уменьшает угрозу подслушивания. Кроме того, риск перехвата можно уменьшить, если пользоваться длинными паролями, которые усложняют их определение из перехваченных сообщений.

Вообще, допускаемая стандартом возможность использования коротких паролей является еще одной причиной уязвимости Bluetooth-соединения, что, как и в случае с использованием простых паролей системными администраторами компьютерных сетей, может привести к их угадыванию (например, при автоматическом сравнении с базой заурядных/распространенных паролей). Такие пароли значительно упрощают инициализацию, но делают ключи связи очень простыми в плане извлечения из перехваченных передач.

Кроме того, ради простоты пользователи склонны применять спаренные ключи связи, а не более защищенные динамичные. По этой же причине вместо комбинаторных ключей они выбирают модульные. А устройство с модульным ключом использует его для соединения со всеми устройствами, которые устанавливают с ним связь. В результате любое устройство с модульным ключом может использовать его для подслушивания на безопасных соединениях, где применяется такой же ключ связи и от проверенных устройств (то есть тех, с которыми связь уже была когда-то установлена). При использовании же модульных ключей никакой защиты не существует.

Однако любое Bluetooth-устройство с личным ключом связи (decryption key) вполне безопасно. Так что меры безопасности по технологии Bluetooth могут защитить соединения только при условии правильной настройки и при правильном пользовании сервисами. И это единственный способ уберечь персональные данные и конфиденциальную информацию от попадания в чужие руки.

# Лекция 11. GSM

### История GSM

В начале 1980-х в Европе, особенно в Скандинавии и Великобритании, а также и во Франции и Германии наблюдался быстрый рост мобильной телефонной связи. Каждая страна разработала свою собственную систему, которая была несовместима со всеми другими в части оборудования и функционирования. Такая ситуация была нежелательна, потому что подвижная аппаратура не только была ограничена функционированием в пределах национальных границ, которых в объединенной Европе было все больше и больше, но очень ограничивало рынок для каждого типа оборудования. Страдали и сбыт, и окупаемость расходов на мобильную связь.

В 1982 г. Конференция европейских почт и телекоммуникаций (CEPT — Conference of European Post and Telecommunication) сформировала группу GSM (Group Special Mobile) для изучения и разработки европейской мобильной наземной системы [42, 104]. Предложенная система должна была соответствовать некоторым критериям:

* хорошее субъективное качество речи;
* низкая стоимость оконечных устройств и обслуживания;
* поддержка международной подвижной связи;
* способность обслуживать малогабаритные терминалы;
* обеспечение диапазона новых услуг и средств;
* эффективное использование радиодиапазона;
* совместимость с ISDN.

В 1989 г. ответственность за разработку GSM была передана Европейскому институту стандартов в области телекоммуникаций (ETSI — European Telecommunication Standards Institute). Первые спецификации GSM были изданы в 1990 г. Коммерческая эксплуатация была начата в середине 1991 г., и к 1993 г. существовало 36 сетей GSM в 22 странах.

Хотя GSM стандартизировано в Европе, это не только европейский стандарт. Сегодня работают более чем 200 сетей GSM (включая DCS-1800 и PCS-1900) в 110 странах во всем мире. В начале 1994 г. во всем мире было 1,3 миллиона абонентов. Сегодня эта цифра выросла до 70 миллионов. Северная Америка имеет разновидность GSM, названную PCS-1900.

Системы GSM существуют теперь на каждом континенте, и сокращение "GSM" (Global System for Mobile Communications) теперь обозначает "Глобальная система для мобильной связи".

Создатели GSM выбрали не опробованную (в то время) цифровую систему, в противоположность применявшимся тогда аналоговым сотовым системам, подобным усовершенствованной системе мобильной связи в Соединенных Штатах (AMPS — Advances Mobile Phone System) и системе с полным доступом (TACS — Total Access Communications System) в Великобритании. Разработчики верили, что усовершенствованные алгоритмы сжатия информации и применение цифровых сигнальных процессоров позволят выполнить поставленные выше задачи и непрерывно совершенствовать систему в смысле качества и стоимости. Более чем 8000 страниц рекомендаций GSM дали возможность построить гибкую и конкурентоспособную систему и обеспечить достаточную стандартизацию, чтобы гарантировать надлежащее межсетевое взаимодействие между компонентами системы, — для этого были созданы описания интерфейсов каждого из функциональных объектов, определенных в системе.

### Услуги, обеспечиваемые GSM

С самого начала разработчики GSM хотели гарантировать совместимость ее с цифровой сетью интегрального обслуживания ISDN в части услуг и передачи сигналов управления. Однако ограничения радиопередачи по пропускной способности и стоимости не позволяли достигнуть стандартной для ISDN скорости передачи информации в битах B-канала 64 Кбит/c.

В соответствии с определением ITU-T (Международного союза электросвязи), телекоммуникационные услуги могут быть разделены на основные и дополнительные услуги. Основная услуга, поддерживаемая GSM, — телефонная связь. Речь закодирована в цифровой форме и передается через сеть GSM как цифровой поток. Существуют также экстренные службы, где, набирая три цифры (например 911), можно получить связь с ближайшим пунктом этой службы.

GSM предоставляет следующие услуги:

1. телефонная связь (совмещается со службой сигнализации: охрана квартир, сигналы бедствия и пр.);
2. передача коротких сообщений;
3. доступ к службам "Видеотекст", "Телетекст";
4. служба "Телефакс" (группа 3).

Пользователи GSM могут обмениваться данными со скоростью свыше 9600 битов в сек.:

* с пользователями обычной телефонной сети (POTS — Plain Ordinary Service);
* с пользователями цифровой сети интегрального обслуживания (ISDN);
* с пользователями сети передачи данных общего пользования с пакетной коммутацией (PSPDN — Packet Switched Public Data Networks);
* с пользователями сети передачи данных общего пользования c коммутацией каналов (CSPDN — Circuit Switched Public Data Networks).

Стандарт GSM предусматривает передачу данных:

* асинхронно в дуплексном режиме со скоростями 300, 600, 1200, 2400, 4800 и 9600 бит/с через телефонные сети общего пользования;
* синхронно в дуплексном режиме со скоростями 1200, 2400, 4800 и 9600 бит/с через телефонные сети общего пользования, коммутируемые сети передачи данных общего пользования (CSPDN) и ISDN;
* в режиме доступа с помощью адаптера к пакетной асинхронной передаче данных со стандартными скоростями 300–9600 бит/с через коммутируемые сети пакетной передачи данных общего пользования (PSPDN);
* в режиме синхронного дуплексного доступа к сети пакетной передачи данных со стандартными скоростями 2400–9600 бит/с.

При передаче данных со скоростью 9,6 Кбит/с всегда задействуется канал связи с полной скоростью передачи. В случае передачи на скоростях ниже 9,6 Кбит/с могут использоваться полускоростные каналы связи.

При этом применяются разнообразные методы доступа и протоколов, таких как X.25 или X.32. Так как GSM — цифровая сеть, между пользователем и сетью GSM не требуется модем, хотя аудиомодем необходим в сети GSM для взаимодействия с обычной телефонной сетью.

Уникальная особенность GSM, которая отсутствует в старых аналоговых системах, — Служба передачи коротких сообщений (SMS — Short Message Service). SMS — двунаправленное обслуживание коротких алфавитно-цифровых (не свыше 160 байтов) сообщений. Сообщения транспортируются способом с промежуточным накоплением (store-and-forward fashion). При соединении между двумя абонентами SMS-сообщение можно передать третьему абоненту и получить подтверждение. SMS может также использоваться в широковещательном режиме, чтобы послать такие сообщения, как модификации трафика или модификации новостей. Сообщения могут также быть сохранены в SIM-карте абонента (SIM — Subscriber Identification Module) для использования в дальнейшем.

Дополнительно стандартизован широкий спектр особых услуг (включение в закрытую группу пользователей, передача вызова, оповещения о тарифных расходах).

Они включают несколько вариантов переадресации вызова и запрет на вызов при входящей и исходящей связи, например, при роуминге (изменении местоположения) в другой стране. Осуществляются такие услуги, как идентификация вызывающего абонента, режим "ждущий вызов", многосторонняя (конференц-) связь.

Важной услугой признается стандарт "закрытой группы". Закрытая группа пользователей (CUG — Closed User Group) — это группа абонентов, в которой устанавливается соединение и происходит обмен информацией преимущественно в пределах этой группы. Возможно предоставление входящей и исходящей связи вне этой группы. При этом абонентам при связи внутри группы предоставляются льготы. Примером такой группы является связь внутри членов одной семьи. Обычно компании сотовой связи предоставляют при такой связи абонентам пониженный тариф или бесплатную связь.

Следующая услуга: сопровождающий вызов обеспечивает переадресацию входящего вызова на номер абонента стационарной сети.

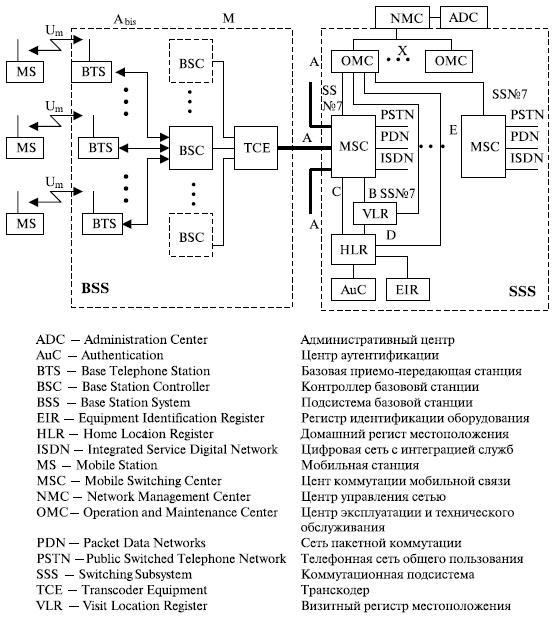
В режиме "ждущий вызов" при занятости абонента входящий вызов ставится в режим ожидания освобождения предыдущего соединения. Абонент, к которому адресован вызов, получает предупреждающий сигнал. Абонент может:

* завершить предыдущий вызов;
* кратковременным нажатием рычага трубки перейти на новое соединение;
* после разговора по новому соединению вернуться к старому и повторить это многократно.

Все перечисленные соединения относятся к группе дополнительных видов обслуживания, которые реализуются в сетях ISDN и современных сетях PSTN.

### Архитектура сети GSM

Сеть GSM состоит из нескольких функциональных объектов, функции и интерфейсы которых показаны на рис. 1.1.



**Рис. 1.1.** Архитектура сети и интерфейсы GSM

Сеть GSM включает три основные части:

* мобильные станции (MS), которые перемещаются с абонентом;
* подсистему базовых станций (BSS), которая управляет радиолинией связи с мобильной станцией;
* подсистему сети (NSS), главная часть которой — центр коммутации мобильной связи (MSC) — выполняет коммутацию между мобильными станциями и между мобильными или стационарными сетевыми пользователями. MSC также управляет работой, связанной с передвижением абонента.

На рис. 1.1 не показан центр обслуживания, который наблюдает за надежным функционированием и изменениями на сети. Мобильная станция (MS) и подсистема базовых станций (BSS) связываются по Um-интерфейсу, также известному как "воздушный интерфейс" или радиолиния связи. Подсистема базовых станций взаимодействует с центром коммутации мобильной связи по A интерфейсу.

#### Мобильная станция

Мобильная станция (MS) состоит из подвижной аппаратуры (терминал) и карты с интегральной схемой, включающей микропроцессор, которая называется модулем абонентской идентификации (SIM — Subscriber Identification Module). SIM-карта обеспечивает при перемещении пользователя доступ к оплаченным услугам независимо от используемого терминала. Вставляя SIM-карту в другой терминал GSM, пользователь может принимать вызовы, делать вызовы с этого терминала и получать другие услуги.

Подвижная аппаратура однозначно определяется с помощью международного опознавательного кода мобильного оборудования (IMEI — International Mobile Equipment Identity). SIM-карта содержит международный опознавательный код мобильного абонента (IMSI — International Mobile Subscriber Identity), используемый для идентификации абонента, секретный код для удостоверения подлинности и другую информацию. IMEI и IMSI независимы — это дает возможность обеспечить наиболее вероятное опознавание личности при передвижении абонента. SIM-карта может быть защищена против неправомочного использования паролем или личным номером.

Применяются три типа оконечного оборудования подвижной станции:

* МТ0 (Mobile Termination 0) — многофункциональная подвижная станция, в состав которой входит терминал данных с возможностью передачи и приема данных и речи;
* МТ1 (Mobile Termination 1) — подвижная станция с возможностью связи через терминал с ISDN;
* МТ2 (Mobile Termination 2) — подвижная станция с возможностью подключения терминала для связи по протоколу МККТТ V-или Х-серий.

Терминальное оборудование может состоять из оборудования одного или нескольких типов, такого как телефонная трубка с номеронабирателем, аппаратура передачи данных (DTE), телекс и т. Д.

Различают следующие типы терминалов: ТЕ1 (Terminal Equipment 1) — терминальное оборудование, обеспечивающее связь с ISDN; ТЕ2 (Terminal Equipment 2) — терминальное оборудование, обеспечивающее связь с любым оборудованием через протоколы МККТТ V- или Х-серий (связь с ISDN не обеспечивает). Терминал ТЕ2 может быть подключен как нагрузка к МТ1 (подвижной станции с возможностью связи с ISDN) через адаптер ТА.

#### Подсистема базовых станций

Подсистема базовых станций содержит два вида оборудования: базовая приемопередающая станция (BTS — Base Transceiver Station) и контроллер базовой станции (BSC — Base Station Controller). Они взаимодействуют через стандартизированный интерфейс Abis (см. рис. 1.1).

На базовой приемопередающей станции размещается приемопередатчик, который для одной определенной соты реализует протоколы радиолинии с передвижной станцией. В большом городе обычно размещено большое количество BTS. Поэтому основные требования к BTS — прочность, надежность, портативность и минимальная стоимость.

Контроллер базовой станции управляет радиоресурсами для одного или более BTS: выбором и установлением соединения по радиоканалу, скачком частоты и хэндовером (переключением), как это будет показано ниже. BSC подключается между базовой приемопередающей станцией (BTS) и центром коммутации мобильной связи (MSC).

#### Коммутационная подсистема сети

##### Центр коммутации мобильный связи (MSC)

Центральный компонент подсистемы сети — центр коммутации мобильной связи (MSC). Он работает как обычный узел коммутации общедоступной телефонной сети (PSTN — Public Switched Telephone Network) или цифровой сети интегрального обслуживания (ISDN — Integrated Service Digital Network). Дополнительно он обеспечивает все функциональные возможности мобильного абонента, такие как регистрация, аутентификация, обновление местоположения, передача соединения (хэндовер) и маршрутизация вызова при передвижении абонента. Эти функции обеспечиваются совместно несколькими функциональными объектами, которые вместе формируют подсистему сети. MSC обеспечивает подключение к фиксированным сетям (таким как общедоступная телефонная сеть PSTN или цифровая сеть интегрального обслуживания ISDN). Передача сигналов между функциональными объектами в подсистеме сети использует ОКС № 7 (SS7) — отдельный канал сигнализации, такой же, как применяется для обмена в ISDN и в сетях общего пользования.

Центр коммутации подвижной связи обслуживает группу сот и обеспечивает все виды соединений, в которых нуждается в процессе работы подвижная станция. MSC аналогичен ISDN коммутационной станции и реализует интерфейс между фиксированными сетями (PSTN, PDN, ISDN и т. д.) и сетью подвижной связи. Он обеспечивает маршрутизацию вызовов и функции управления вызовами. Кроме выполнения функций обычной ISDN коммутационной станции на MSC возлагаются функции коммутации радиоканалов. К ним относятся "эстафетная передача", в процессе которой достигается непрерывность связи при перемещении подвижной станции из соты в соту, и переключение рабочих каналов в соте при появлении помех или неисправностях.

Каждый MSC обеспечивает обслуживание подвижных абонентов, расположенных в пределах определенной географической зоны (например, Москва и область). MSC управляет процедурами установления вызова и маршрутизации. Для телефонной сети общего пользования (PSTN) MSC обеспечивает функции сигнализации по протоколу ОКС №7, передачи вызова или поддержки других видов интерфейсов в соответствии с требованиями конкретного проекта.

MSC формирует данные, необходимые для выписки счетов за предоставленные сетью услуги связи, накапливает данные по состоявшимся разговорам и передает их в центр расчетов (биллинг-центр). MSC составляет также статистические данные, необходимые для контроля работы и оптимизации сети. Он же поддерживает процедуры безопасности, применяемые для управления доступами к радиоканалам.

MSC не только участвует в управлении вызовами, но также управляет процедурами регистрации местоположения и передачи управления, кроме передачи управления в подсистеме базовых станций (BSS). Регистрация местоположения подвижных станций необходима для обеспечения доставки вызова перемещающимся подвижным абонентам от абонентов телефонной сети общего пользования или других подвижных абонентов. Процедура передачи вызова позволяет сохранять соединения и обеспечивать ведение разговора, когда подвижная станция перемещается из одной зоны обслуживания в другую. Передача вызовов в сотах, управляемых одним контроллером базовых станций (BSC), осуществляется этим BSC. Когда передача вызовов происходит между двумя сетями, управляемыми разными BSC, то первичное управление осуществляется в MSC. В стандарте GSM также предусмотрены процедуры передачи вызова между сетями (контроллерами), относящимися к разным MSC. Центр коммутации осуществляет постоянное слежение за подвижными станциями, используя домашний регистр местоположения (HLR) и визитный регистр местоположения (VLR).

##### Домашний регистр местоположения (HLR — Home Location Register)

В HLR хранится та часть информации о местоположении какой-либо подвижной станции, которая позволяет центру коммутации доставить вызов определенной мобильной станции. Практически HLR представляет собой справочную базу данных о постоянно зарегистрированных в сети абонентах. В ней содержатся опознавательные номера и адреса, а также параметры подлинности абонентов, состав услуг связи, специальная информация о маршрутизации. Ведется регистрация данных об изменении местоположения и роуминге ("блуждании") абонента, включая данные о временном идентификационном номере подвижного абонента (TMSI — Temporary Mobile Subscriber Identity) и соответствующем визитном регистре местоположения (VLR). Регистр HLR содержит международный идентификационный номер подвижного абонента (IMSI — International Mobile Subscriber Identity), состав услуг связи, специальную информацию о маршрутизации. Он используется для опознавания подвижной станции в центре аутентификации (AUC — Authentication Center).

Домашний регистр местоположения (HLR ) вместе с MSC обеспечивает маршрутизацию вызова и изменения местоположения (роуминг) мобильной станции и содержит всю административную информацию каждого абонента, зарегистрированного в соответствующей сети GSM, наряду с текущим местоположением мобильных станций. Местоположение мобильных станций находится обычно в форме адреса данной мобильной станции в VLR. Фактическая процедура маршрутизации будет описана позже. Логически существует только один HLR в сети GSM, хотя он может быть реализован как распределенная база данных. К данным, содержащимся в HLR, имеют дистанционный доступ все MSC и VLR сети, и, если в сети имеются несколько HLR, в базе данных содержится только одна запись об абоненте, поэтому каждый HLR представляет собой определенную часть общей базы данных сети об абонентах. Доступ к базе данных об абонентах осуществляется по номеру IMSI (IMSI — International Mobile Station Identity) или по MSISDN-номеру подвижной станции в сети ISDN (MSISDN — Mobile Station ISDN Number). К базе данных могут получить доступ MSC или VLR, относящиеся к другим сетям, в рамках обеспечения межсетевого роуминга абонентов.

##### Визитный регистр местоположения (VLR — Visit Location Register)

### Второе основное устройство, обеспечивающее контроль над передвижением подвижной станции из зоны в зону, — визитный регистр местоположения VLR. С его помощью достигается функционирование подвижной станции за пределами зоны, контролируемой HLR. Когда в процессе перемещения подвижная станция переходит из зоны действия одного контроллера базовой станции BSC, объединяющего группу базовых станций, в зону действия другого BSC, она регистрируется новым BSC, и в VLR заносится информация о номере области связи, которая обеспечит доставку вызовов подвижной станции. Для сохранности данных, находящихся в HLR и VLR, в случае сбоев предусмотрена защита устройств памяти этих регистров.

### VLR включает в себя такие же данные, как и HLR, однако эти данные содержатся в VLR только до тех пор, пока абонент находится в зоне, контролируемой VLR.

### В сети подвижной связи GSM соты группируются в географические зоны (LA — Location Area), которым присваивается свой идентификационный номер (LAC — Location Area Code). Каждый VLR содержит данные об абонентах в нескольких LA. Когда подвижный абонент перемещается из одной LA в другую, данные о его местоположении автоматически обновляются в VLR. Если старая и новая LA находятся под управлением различных VLR, то данные на старом VLR стираются после их копирования в новый VLR. Текущий адрес VLR абонента, содержащийся в HLR, также обновляется.

### VLR обеспечивает также присвоение номера для услуг роуминга мобильной станции (MSRN — Mobile Station Roaming Number). Когда подвижная станция принимает входящий вызов, VLR выбирает его MSRN и передает его на MSC, который осуществляет маршрутизацию этого вызова к базовым станциям, находящимся рядом с подвижным абонентом.

### Во время движения подвижная станция может покинуть зону, обслуживаемую одним MSC/VLR, и переместиться в зону, которую обслуживает другой MSC/VLR. В этом случае MSC/VLR участвует в передаче управления от одного MSC/VLR к другому. Он также присваивает новый временный мобильный опознавательный код станции TMSI (Temporary Mobile Subscriber Identity) и передает его в HLR. Новый MSC/VLR инициирует процедуру установления подлинности абонента и его оборудования. Кроме случая, когда подвижный абонент меняет зону местоположения, временный номер может периодически изменяться по решению оператора с целью защиты от злонамеренного перехвата номеров участников разговора. В этом случае процедура изменения идет также с использованием VLR, для доступа к VLR могут использоваться идентификационные номера IMSI, TMSI и MSRN.

### В заключение отметим, что VLR — это локальная база данных в данной зоне, которая содержит информацию о подвижном абоненте. Применение VLR позволяет сократить число запросов HLR, и это снижает сетевой трафик и уменьшает время обслуживания.

### Cостав долговременных и временных данных, хранящихся в HLR и VLR.

1. Международный идентификационный номер подвижного абонента (IMSI- International Mobile Subscriber Identity)
2. Номер подвижной станции в сети ISDN (MSISDN)
3. Категория подвижной станции
4. Ключ засекречивания
5. Используемые пароли
6. Класс приоритетного доступа
7. Список разрешенных дополнительных видов обслуживания
8. Оповещение вызываемого абонента о номере вызывающего абонента
9. Разрешение/запрещение идентификации номера вызываемого абонента
10. График работы мобильной станции
11. Индекс закрытой группы пользователей
12. Код блокировки закрытой группы пользователей
13. Состав вызовов, которые могут быть переданы
14. Свойства закрытой группы пользователей
15. Льготы закрытой группы пользователей
16. Запрещенные исходящие вызовы в закрытой группе пользователей
17. Максимальное количество абонентов закрытой группы
18. Временный номер подвижного абонента в VLR (TMSI- Temporary Mobile Subscriber Identity)
19. Параметры аутентификации и шифрования
20. Адрес регистра местоположения VLR
21. Код Зоны Местоположения
22. Номер соты при хэндовере
23. Регистрационные данные
24. Таймер ожидания ответа
25. Состав текущих паролей
26. Активность (есть/нет соединения)
27. Временный идентификационный номер подвижного абонента (TMSI – Temporary Mobile Subscriber Identity)
28. Идентификаторы зоны расположения
29. Код Зоны Местоположения
30. Номер соты при хэндовере
31. Параметры аутентификации и шифрования

##### Регистры защиты и аутентификации

### Для защиты и аутентификации используются два устройства: регистр идентификации оборудования (EIR — Equipment Identity Register) и центр аутентификации (AUC — Authentication Center). Регистр идентификации оборудования — база данных, которая содержит список всей допустимой к обслуживанию подвижной аппаратуры на сети, где каждая мобильная станция идентифицирована ее международным опознавательным кодом мобильного оборудования (IMEI). IMEI может быть маркирован как запрещенный к обслуживанию, если станция украдена или такого типа, который не обслуживается. Центр аутентификации — защищенная база данных, которая накапливает копии ключей засекречивания, хранящихся в SIM-карте каждого абонента, и используется для аутентификации абонента и его оборудования, а также и шифрования для передачи по радиоканалу.

### Каждый подвижный абонент имеет стандартный модуль подлинности абонента (SIM), который содержит: международный идентификационный номер (IMSI), свой индивидуальный ключ аутентификации (Ki), алгоритм аутентификации (A3).

### С помощью записанной в SIM информации в результате взаимного обмена данными между подвижной станцией и сетью осуществляется полный цикл аутентификации и разрешается доступ абонента к сети.

### EIR — регистр идентификации оборудования, содержит централизованную базу данных для подтверждения подлинности международного идентификационного номера оборудования подвижной станции (IMEI). Эта база данных относится исключительно к оборудованию подвижной станции. Она состоит из списков номеров IMEI, организованных следующим образом.

### БЕЛЫЙ СПИСОК содержит номера IMEI, о которых есть сведения, что они закреплены за санкционированными подвижными станциями. Терминалу позволяют соединиться с сетью.

### ЧЕРНЫЙ СПИСОК содержит номера IMEI подвижных станций, которые украдены, имеют некорректный тип мобильной станции для сети GSM или им отказано в обслуживании по другой причине. Терминалу не позволяют соединиться с сетью.

### СЕРЫЙ СПИСОК содержит номера IMEI подвижных станций, у которых существуют проблемы, выявленные по данным программного обеспечения, но не являющиеся основанием для внесения в "черный список". Терминал находится под наблюдением сети ввиду возможных проблем.

### К базе данных EIR получают дистанционный доступ MSC данной сети, а также MSC других подвижных сетей.

### Как и в случае с HLR, сеть может иметь более одного EIR, при этом каждый EIR управляет определенной группой оборудования, имеющей свой идентификационный номер IМЕI. В состав MSC входит транслятор, который при получении номера IМЕI выбирает адрес EIR — он содержит данные о части оборудования, имеющей этот номер.

##### Оборудование эксплуатации и технического обслуживания

### ОМС (Operations and Maintenance Center) — центр эксплуатации и технического обслуживания, является центральным элементом сети GSM, который обеспечивает контроль и управление другими компонентами сети, а также контроль качества ее работы. ОМС соединяется с другими компонентами сети GSM по каналам пакетной передачи протокола Х.25. Он обеспечивает функции обработки аварийных сигналов, предназначенных для оповещения обслуживающего персонала, и регистрирует сведения об аварийных ситуациях в других компонентах сети. В зависимости от характера неисправности ОМС позволяет обеспечить ее устранение автоматически или при активном вмешательстве персонала. Центр может провести проверку состояния оборудования сети и прохождения вызова подвижной станции. ОМС позволяет производить управление нагрузкой в сети. Функция эффективного управления включает сбор статистических данных о нагрузке от компонентов сети GSM, запись их в дисковые файлы и вывод на дисплей для визуального анализа. ОМС обеспечивает управление изменениями программного обеспечения и базами данных о конфигурации элементов сети. Загрузка программного обеспечения в память может производиться из ОМС в другие элементы сети или из них в ОМС.

### NMC (Network Management Center) — центр управления сетью, дает возможность рационального иерархического управления сетью GSM. Он обеспечивает эксплуатацию и техническое обслуживание на уровне всей сети, поддерживаемой центрами ОМС, которые отвечают за управление региональными сетями. NMC отвечает за управление трафиком во всей сети и обеспечивает диспетчерское управление сетью при сложных аварийных ситуациях, как, например, выход из строя или перегрузка узлов. Кроме того, он контролирует состояние устройств автоматического управления, задействованных в оборудовании сети, и отражает на дисплее состояние сети для операторов NMC. Это позволяет операторам контролировать региональные проблемы и при необходимости оказывать помощь ОМС, обслуживающему конкретный регион. Таким образом, персонал NMC знает состояние всей сети и может дать указание персоналу ОМС изменить стратегию решения региональной проблемы.

### NMC следит за состоянием маршрутов сигнализации и соединений между узлами, чтобы не допускать условий для возникновения перегрузки в сети. Контролируются также маршруты соединений между сетью GSM и PSTN во избежание распространения условий перегрузки между сетями. При этом персонал NMC координирует вопросы управления сетью с персоналом других NMC. NMC обеспечивает также возможность управления трафиком для сетевого оборудования подсистемы базовых станций (BSS). Операторы NMC в экстремальных ситуациях могут задействовать такие процедуры управления, как "приоритетный доступ", когда только абоненты с высоким приоритетом (экстренные службы) могут получить доступ к системе.

### NMC может брать на себя ответственность в каком-либо регионе, когда местный ОМС не способен обслуживать нагрузку, при этом ОМС действует в качестве транзитного пункта между NMC и оборудованием сети. NMC обеспечивает операторов функциями, аналогичными функциям ОМС.

### NMC является также важным инструментом планирования сети, так как контролирует сеть и ее работу на сетевом уровне, а следовательно, снабжает планировщиков сети данными, определяющими нагрузочные параметры сети.

### ADC (Administration Center) — административный центр — сетевая служба, ответственная за организацию связи, административное управление сетью и соблюдение установленных правил доступа.

### ТСЕ (Transcoder Equipment) — транскодер, обеспечивает преобразование выходных сигналов передачи речи и данных MSC (64 Кбит/с ИКМ) к виду, соответствующему рекомендациям GSM по радиоинтерфейсу. В соответствии с этими требованиями скорость передачи речи, представленной в цифровой форме, составляет 13 Кбит/с. Этот канал передачи цифровых речевых сигналов называется "полноскоростным". Стандартом предусматривается в перспективе использование полускоростного речевого канала (скорость передачи 6,5 Кбит/с).

### Снижение скорости передачи обеспечивается применением специального речепреобразующего устройства, использующего кодирование с линейным предсказанием (LPC — Linear Predictive Coding), долговременное предсказание (LTP — Long Term Predicting), возбуждение регулярной импульсной последовательностью (RPE — иногда называется RELP).

### Транскодер обычно располагается вместе с MSC. Передача цифровых сообщений по направлению к контроллеру базовых станций (BSC) ведется с добавлением к потоку со скоростью передачи 13 Кбит/с дополнительных битов (stuffing). Таким образом, скорость передачи данных становится 16 Кбит/с. Затем осуществляется уплотнение с кратностью 4 в стандартный канал 64 Кбит/с. Так формируется определенная рекомендациями GSM

### З0-канальная ИКМ линия, обеспечивающая передачу 120 речевых каналов. Шестнадцатый канал (64 Кбит/с) (slot) выделяется отдельно для передачи информации сигнализации и часто содержит сигналы ОКС № 7 или процедуры доступа к звену передачи данных для канала "D" — LAPD (Link Access Procedure for the D - channel).

### В других каналах (64 Кбит/с) могут передаваться также пакеты данных, согласующиеся с протоколом X.25 МККТТ.

### Основные принципы организации сети GSM

#### Внутренние интерфейсы GSM

#### Внутренние интерфейсы [22, 27, 32, 49] показаны на рис. 1.1 и перечислены в табл. 1.4.

|  |  |
| --- | --- |
| Тип | Связь между устройствами |
| A | MSC-BSS |
| Abis | BSC-BTS |
| B | MSC-VLR |
| C | MSC-HLR |
| D | HLR-VLR |
| E | MSC-MSC |
| O | BSC-OMC |
| M | BSC-TCE |
| Um | MS-BTS |
| X | OMC-OMC |

#### Примечание: X-интерфейс предназначен для связи OMC различных GSM

#### А-интерфейс. Интерфейс между MSC и BSS (подсистема базовых станций –BSC- BTS) обеспечивает передачу сообщений для управления BSS, передачи вызова (хэндовер), управления при изменении местоположения. А-интерфейс объединяет каналы связи и линии сигнализации. Последние используют протокол ОКС № 7 МККТТ. Полная спецификация A-интерфейса соответствует требованиям серии 08 Рекомендации ETSI/GSM.

#### Abis-интерфейс. Интерфейс служит для связи между BSC с BTS и определен Рекомендациями ETSI/GSM для процессов установления соединений и управления оборудованием, передача осуществляется цифровыми потоками со скоростью 2,048 Мбит/с. Возможно использование физического интерфейса 64 Кбит/с.

#### В-интерфейс. Интерфейс между MSC и VLR. Когда MSC необходимо определить местоположение подвижной станции, он обращается к VLR. Если подвижная станция инициирует процедуру изменения местоположения, то MSC информирует свой VLR, который заносит всю изменяющуюся информацию в свои регистры. Эта процедура происходит всегда, когда MS переходит из одной области в другую. В случае если абонент запрашивает специальные дополнительные услуги или изменяет некоторые свои данные, MSC также информирует VLR, который регистрирует изменения и при необходимости сообщает о них HLR.

#### С-интерфейс. Интерфейс используется для обеспечения взаимодействия между MSC и HLR. MSC может послать сообщение HLR в конце сеанса связи для того, чтобы абонент мог оплатить разговор. Когда сеть фиксированной телефонной связи не способна выполнить процедуру установления соединения подвижного абонента, MSC может запросить HLR с целью определения местоположения абонента, чтобы послать вызов MS.

#### D-интерфейс. Интерфейс между HLR и VLR используется для расширения обмена данными о положении подвижной станции и управления процессом связи. Основные услуги, предоставляемые подвижному абоненту, заключаются в возможности передавать или принимать сообщения независимо от местоположения. Для этого HLR должен пополнять свои данные. VLR сообщает HLR о положении MS, управляя ею и изменяя информацию в процессе обновления местоположения, а также посылает все необходимые данные для обеспечения обслуживания подвижной станции.

#### Е-интерфейс. Интерфейс обеспечивает взаимодействие между разными MSC при осуществлении процедуры handover — "передачи" абонента из зоны в зону при его движении в процессе сеанса связи без ее перерыва.

#### О-интерфейс. Интерфейс между BSC и ОМС предназначен для связи BSC с ОМС, используется в сетях с пакетной коммутацией МККТТ Х.25.

#### M-интерфейс. Внутренний BSC-интерфейс контроллера базовой станции обеспечивает связь между различным оборудованием BSC и оборудованием транскодирования (ТСЕ); использует стандарт ИКМ-передачи 2,048 Мбит/с и позволяет организовать из четырех каналов со скоростью 16 Кбит/с один канал на скорости 64 Кбит/с.

#### Um-радиоинтерфейс. Интерфейс между MS и BTS определен в сериях 04 и 08 Рекомендаций ETSI/GSM [76–79].

#### X-интерфейс. Сетевой интерфейс между ОМС разных сетей и так называемый управляющий интерфейс между ОМС и элементами сети, определен ETSI/GSM Рекомендациями 12.01 и является аналогом интерфейса Q.3, который определен в многоуровневой модели открытых сетей ISO OSI.

#### Соединение сети с ОМС могут обеспечиваться системой сигнализации МККТТ ОКС №7 или сетевым протоколом Х.25. Сеть Х.25 может соединяться с объединенными сетями или с PSDN в открытом или замкнутом режимах.

#### GSM-протокол управления сетью и обслуживанием также должен удовлетворять требованиям Q.3 интерфейса, который определен в ETSI/GSM Рекомендациях 12.01.

#### 1.4.2. Интерфейсы с внешними сетями

#### Соединение с PSTN

#### Соединение с телефонной сетью общего пользования осуществляется MSC по линии связи 2 Мбит/с в соответствии с системой сигнализации ОКС № 7. Электрические характеристики 2 Мбит/с интерфейса соответствуют Рекомендациям МККТТ G.732.

#### Соединение с ISDN

#### Для соединения с создаваемыми сетями ISDN предусматриваются четыре линии связи 2 Мбит/с, поддерживаемые системой сигнализации ОКС №7. Система сигнализации ОКС № 7 будет рассмотрена в дальнейшем.

#### Соединения с международными сетями GSM

#### В настоящее время обеспечивается подключение сети российской сети GSM к общеевропейским сетям GSM. Эти соединения осуществляются на основе протоколов систем сигнализации ОКС№7 четвертого уровня (SCCP — Signaling Connection Control Part) и межсетевого коммутационного центра мобильной связи (GMSC — Gateway MSC). Центр представляет узловую станцию, осуществляющую объединение сети GSM с одной или более наземными сетями. В ее функции входит преобразование форматов сигналов, конвертирование сетевых протоколов, а также взаимодействие с ТфОП.

#### Географические зоны сети GSM

#### Сеть GSM составлена из географических областей [81]. Как показано на рис. 1.2, эти области включают ячейки, зоны местоположения (LA's — Location Areas), зоны обслуживания MSC/VLR и мобильную наземную сеть общего пользования (PLMN — Public Land Mobile Network).

#### Сота — область радиоохвата одного приемопередатчика одной BTS. Сеть GSM определяет каждую соту с помощью опознавательного кода глобального идентификатора соты (CGI — Cell Global Identity), номера, который назначается каждой соте.

#### Зона местоположения (LA — Location Area) — группа сот. Это область, в которой вероятнее всего может в данный момент перемещаться абонент.

#### 

#### 

#### Рис. 1.2. Географические зоны системы GSM

#### Каждая зона местоположения обслуживается одним или более контроллерами базовых станций и только единственным центром коммутации мобильной связи — MSC (см. рис. 1.2). Каждой зоне местоположения (LA) назначен идентификатор зоны нахождения абонента (LAI — Location Area Identification).

#### Зона обслуживания MSC/VLR представляет собой часть сети GSM, которая обслуживается одним MSC и зарегистрирована в VLR данного MSC ( рис. 1.3).

#### Мобильная наземная сеть общего пользования (PLMN — Public Land Mobile Network) — это совокупность зон обслуживания, принадлежащих одному сетевому оператору.

#### 

#### 

#### Рис. 1.3. Зона местоположения (LA)

#### 

#### 

#### Рис. 1.4. Мобильная наземная сеть (PLMN)

#### 1.4.4. Повторное использование частот (Frequency reuse)

#### Повторное использование частот — способ организации связи, при котором одни и те же частоты многократно используются в разных зонах обслуживания [27, 32, 49, 101]. Применение частотно-территориального планирования с повторным использованием частот позволяет увеличить пропускную способность при ограниченном количестве частотных каналов.

#### Расстояние повторного использования частот (Frequency reuses distance) — расстояние между центрами двух удаленных сот, начиная с которого допускается повторное использование. В общем случае оно определяется по формуле , где — число ячеек в кластере, — радиус ячейки (радиус окружности, описанной вокруг гексагональной ячейки).

#### Кластер (cluster). Кластер — это группа из близко расположенных сот, в пределах которых недопустимо повторное использование из-за опасности превышения уровня взаимных помех. Размер кластера определяется по формуле:

#### 

#### Из этой формулы видно, что кластер может содержать только определенное число сот.

#### При:

#### i=0, j=1, N=1; i=1, j=1, N=3; i=1, j=2, N=4; и т. д.

#### Приведенное соотношение для показывает, что чем меньше радиус ячейки , тем выше коэффициент повторяемости частот ( ), а следовательно, и эффективность использования выделенного диапазона частот. Отношение называется коэффициентом снижения внутриканальных помех и характеризует степень взаимного влияния удаленных сот, в которых используются одни и те же частотные каналы. Для приведенных выше значений значение равно: .

#### Пример распределений частот при повторном использовании показан на [рис. 1.5](http://www.intuit.ru/studies/courses/551/407/lecture/5214?page=4#image.1.5) (4-элементный кластер) и [рис. 1.6](http://www.intuit.ru/studies/courses/551/407/lecture/5214?page=4#image.1.6) (7-элементный кластер).

#### 

#### 

#### Рис. 1.5. Повторное использование частот при 4-элементном кластере

#### 

#### 

#### Рис. 1.6. Повторное использование частот при 7-элементном кластере

#### Секторизованная сота

Сота, в которой обслуживание абонентов осуществляется базовой станцией с секторной антенной, называется секторизованной сотой. При этом зона покрытия антенны разделяется на секторы. Секторизация позволяет повысить пропускную способность системы сотовой связи без уменьшения размеров зоны покрытия или снижения мощности, излучаемой базовой станцией. Ширина направленности секторной антенны соответствует угловому размеру сектора. В системах сотовой связи обычно используют антенны с шириной диаграммы направленности 120° (трехсекторная антенна). Обычно применяются кластеры размерностью 3/9, 4/12, 7/21, где первая цифра обозначает число сот в кластере, а вторая — число секторов. На рис. 1.7-а показан пример применения 3-секторной антенны для кластера 3/9. В этом примере распределяются 9 групп частот и применяются шестисекторные антенны — с шириной диаграммы направленности 60°. На рис. 1.7-б показана разработанная корпорацией Motorola сотовая сеть с шириной одного из вариантов диаграммы направленности 60° и 12 группами несущих частот [22]. Этот кластер содержит 4 элемента и 6-секторную антенну (размер кластера 4/24).



**Рис. 1.7.** Повторное использование частот в: а) 3-секторной соте; б) 6-секторной соте

#### Задачи каналов в системе GSM

Очевидно, что использование радиоканалов в мобильной сети GSM отличается от их применения в стационарной сети. Принцип использования каналов в системе GSM показан на рис. 1.8.

В стационарной сети абонентские линии (абонентские каналы трафика) закреплены за телефонным аппаратом. Когда известен номер абонента, то при исходящей или входящей связи не требуется выбор абонентской линии.

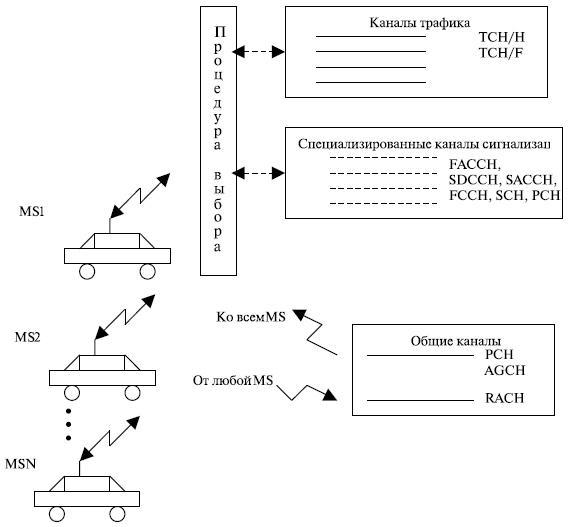
В сети GSM определены два типа каналов трафика: полноскоростные речевые каналы, работающие на полной скорости (TCH/F — Traffic Channel/Full) — 22,8 Кбит/с, и полускоростные речевые каналы, работающие на половинной скорости (TCH/H — Traffic Channel/Half) — 11,4 Кбит/с. Половинная скорость позволяет вдвое увеличить число каналов в одном и том же частотном диапазоне.

В мобильной связи каналы трафика доступны любому абоненту. Поэтому в процессе установления соединения может быть выбран любой канал, к которому может быть подключена станция. Поскольку в свободном состоянии абонентская линия не имеет связи с каналами трафика, она нуждается в канале управления, например, для передачи сигнала "вызов", "setup", номера вызывающего абонента и т. п.

Поэтому для передачи запроса сети на установление соединения применяется канал, направленный от MS к сети. Это канал случайного доступа (RACH — Random Access Control Channel).

Поскольку запрос на установление соединения передается только в начале соединения и в дальнейшем выделяется канал для обмена управляющей информацией, этот канал является общим для всех станций зоны местонахождения.

Общему каналу всегда требуется процедура доступа для избежания и разрешения конфликтов. В данном случае чаще всего применяется процедура случайного многостанционного доступа с временным разделением типа ALOHA (TDMA — Time Division Multiple Access ALOHA). Принцип такого доступа основан на том, что все станции используют один канал связи, контролируя его работу, а передача осуществляется в случайные моменты времени, что уменьшает вероятность конфликтов. Такой доступ подробно описан в курсе лекций "Абонентские оконечные устройства и сети доступа".



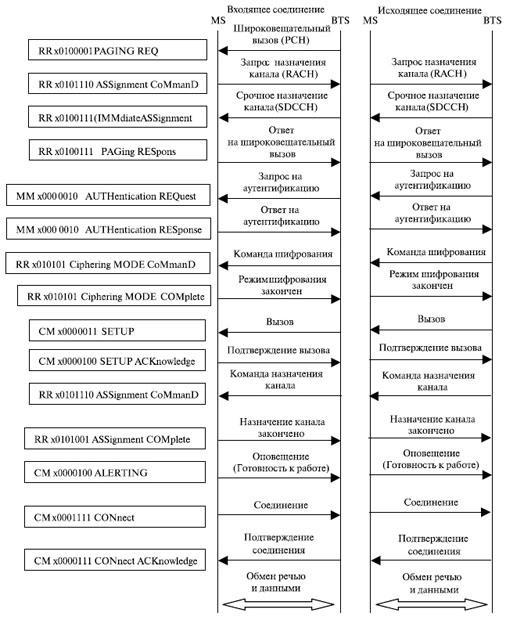
**Рис. 1.8.** Принцип использования каналов трафика и сигнальных каналов в системе GSM

В ответ на сигнал вызова выбирается автономный специализированный канал управления (SDCCH — Stand-alone dedicated Control Channel), по которому в дальнейшем передается служебная информация от MS в течение установления вызова прежде, чем будет найден канал трафика (TCH).

Для входящей связи передача сигнала "занятие" к MS реализуется по широковещательному каналу коротких сообщений (канал вызова) (PCH — Paging Channel), общему для всей соты. Это широковещательный канал коротких сообщений, который передает сигнал "вызов" всем станциям зоны местоположения (LA). Получив такой сигнал, станция MS определяет свой номер и отвечает на широковещательный сигнал так же, как при исходящем вызове, — сигналом запроса по каналу случайного доступа (RACH — Random Control Channel).

Далее сигналы установления соединения проходят как и при исходящей связи.

Порядок обмена сигналами для входящего и исходящего соединения приведен на рис. 1.9.



**Рис. 1.9.** Порядок обмена сигналами для входящего и исходящего соединения

На рисунке показаны некоторые особенности передачи сигналов. Ниже даны некоторые пояснения. Нарисованные слева коды сигналов будут рассмотрены далее.

При входящей связи BTS и MS пункта назначения (работа других элементов сети на данном рисунке не изображается):

1. передает широковещательный сигнал всем станциям в зоне обслуживания данного MSC. Сигнал передается по отдельному каналу управления - широковещательному каналу коротких сообщений — РСН (Paging Channel);
2. после чего MS по каналу управления (канал со случайным доступом — RACH, Random Access Channel) посылает запрос на срочное назначение индивидуального канала управления на время обмена сигналами. Слова "произвольный доступ" означают применение методов случайного доступа, наиболее распространенным из которых является ALOHA (см. курс лекций "Абонентские оконечные устройства и сети доступа"). Принцип работы при таком методе заключается в том, что все станции работают по одному каналу связи, контролируя его работу, передача осуществляется в случайный момент времени. BTS выбирает канал для обмена управляющими сигналами (SDCCH — Stand-alone dedicated Control Channel);
3. BTS запрашивает данные аутентификации. Проводится аутентификация с помощью данных, полученных ранее при реализации процедуры аутентификации и защиты пользователя. В ответ на запрос MS передает накопленный в SIM-карте зашифрованный отклик (SRES — Signed Response), что позволяет BTS установить подлинность MS;
4. после чего BTS передает запрос ключа шифрования;
5. и получает ответный ключ шифрования. Если ключ правильный, то далее проводится процедура установления соединения, которая совпадает с процедурой исходящего соединения.

Теперь можно рассмотреть подробнее весь состав сигнальных каналов.

#### Каналы сигнализации радиоинтерфейса

Сигнальные каналы радиоинтерфейса используются для установления вызова, широковещательной рассылки коротких сообщений (paging), технического обслуживания вызова, синхронизации и т. д. ( рис. 1.10).



**Рис. 1.10.** Состав каналов радио интерфейса системы GSM

Имеется 3 группы сигнальных каналов

**Широковещательные каналы (BCH — Broadcast Channel)**. Доставляют информацию от станции к абоненту (downstream) и предназначены главным образом для коррекции частоты и синхронизации. Это единственный тип канала, допускающий связь "от точки — ко многим точкам", при которой короткие сообщения могут быть переданы одновременно нескольким мобильным телефонам.

BCH включают следующие каналы:

* широковещательный канал управления (BCCH — Broadcast Control Channel). Общая информация, касающаяся сот; например, код зоны местоположения (LAC — Location Area Code), сетевой оператор, доступ, параметры, список соседних ячеек и т. д. MS получают сигналы через BCCH от многих BTS в пределах той же самой сети или различных сетей;
* канал подстройки частоты (FCCH — Frequency Correction Channel). Канал связи от сети к MS, предназначенный только для коррекции частот MS и передачи частоты к MS. Он также используется для вхождения в синхронизм, обеспечивая соблюдение заданной дистанции между временными интервалами и позицией первого временного интервала кадра TDMA (множественного доступа с временным уплотнением);
* канал синхронизации (SCH — Synchronizing Channel). Исходящий канал от MS к сети; отвечает за синхронизацию кадра TDMA и идентификацию базовой станции. SCH обеспечивает MS всей информацией, необходимой для синхронизации с BTS.

**Общие каналы управления (CCCH — Common Control Channels)**: группа канала связи от абонента к станции и каналы связи от сети к MS. Эти каналы используются, чтобы передать информацию между сетью и MS. Общие каналы управления CCCH включают следующие каналы:

* широковещательный канал коротких сообщений (канал вызова) (PCH — Paging Channel): исходящий канал только от сети к MS; BTS информирует MS о входящих вызовах через PCH;
* канал предоставления доступа (AGCH): исходящий канал только от сети к MS. BTS распределяет TCH или SDCCH к MS, таким образом разрешая MS доступ к сети;
* канал с произвольным доступом (RACH): канал связи только от MS к сети; позволяет MS запрашивать SDCCH. Это делается в ответ на широковещательный запрос или на вызов. MS для передачи на этом канале работает по принципу случайного доступа.

PCH и AGCH передают информацию в одном канале, называемую широковещательным сообщением, и каналом предоставления доступа, как это будет показано далее.

**Специализированные каналы управления (DCCH — Dedicated Control Channel)**. Предназначены, например, для обслуживания: роуминга, изменения местоположения, передачи соединения (хэндовер), шифрования и т. д.

DCCH включают следующие каналы:

* автономный выделенный канал управления (SDCCH — Stand-Alone Dedicated Control Channel): канал, соединяющий MS и BTS, для передачи сигналов в течение установления вызова прежде, чем будет найден канал трафика (TCH);
* низкоскоростной совмещенный канал управления (SACCH — Slow Associated Control Channel): передает непрерывные сообщения об измерениях (например, напряженность поля). Параллельно с ним могут работать TCH или SDCCH необходим, например, для решений хэндовера; применяется подобно TCH или SDCCH для несрочных процедур, например, для измерения радиосигналов, управления мощностью (только исходящий канал от сети к MS);
* быстродействующий объединенный канал управления (FACCH — fast associated control channel): его функции сродни SDCCH, но он может использоваться временно для работы как TCH в режиме перераспределения каналов (borrowing mode) совместно с SDCCH, если скорость данных SDCCH (низкоскоростного выделенного канала управления) недостаточна.

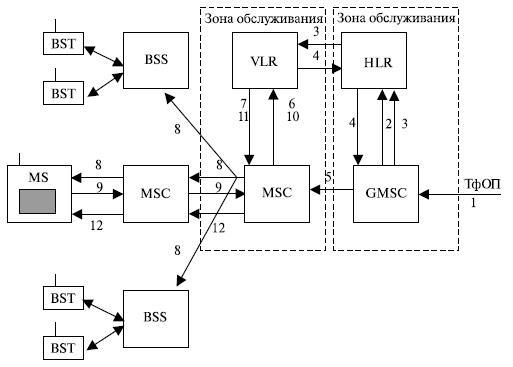
Дополнительная пропускная способность применяется, например, для процедур, связанных с установлением подлинности (аутентификацией), установлением соединения, хэндовером и т. д.

Почти все сигнальные каналы используют формат нормального пакета, кроме RACH (пакет произвольного доступа), FCCH (пакет коррекции частоты) и SCH (пакет синхронизации).

#### Некоторые примеры работы сети GSM

##### Обслуживание вызова от абонента стационарной сети к абоненту мобильной сети GSM

Cледующий пример [33, 36, 40, 81, 84, 86, 98, 107] описывает обслуживание вызова от абонента стационарной сети к абоненту мобильной сети GSM ( рис. 1.11):

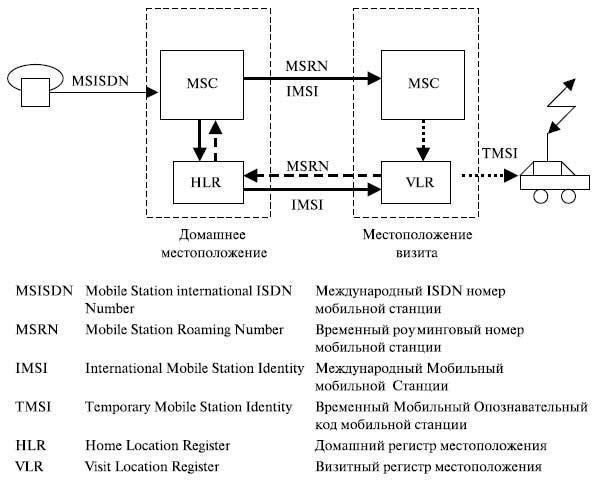


**Рис. 1.11.** Обслуживание вызова от абонента стационарной сети к абоненту мобильной сети GSM

В рассматриваемом примере порядок действий следующий:

1. Входящий вызов поступает от стационарной сети ТфОП на вход шлюза MSC (GMSC — Gateway MSC).
2. На основе международного мобильного идентификационного номера станции (IMSI — International Mobile Station Identity) вызываемого абонента определяется домашний регистр местоположения (HLR).
3. Затем запрашивают соответствующий визитный регистр местоположения (VLR) для того, чтобы определить для мобильной станции номер для услуг роуминга ( рис. 1.12) — MSRN (Mobile Station Roaming Number).
4. Он передается назад в HLR GMSC.
5. Затем соединение переключается к соответствующему MSC.
6. MSC вырабатывает запрос VLR.
7. Теперь визитный регистр местоположения (VLR) делает запрос зоны местоположения (LA — Location Area) и о состоянии (доступности) мобильного абонента. Если MS отмечена как доступная, то выполняется п. 8.
8. Передается широковещательный вызов по всей зоне нахождения, записанной в визитном регистре местоположения (VLR).
9. Мобильный абонентский телефон отвечает на широковещательный запрос из текущей радиосоты.
10. После этого выполняются все необходимые процедуры безопасности (аутентификация и обмен шифровальными ключами). Если они выполнены успешно, то выполняется п. 11.
11. Визитный регистр местоположения (VLR) указывает для MSC, что вызов закончен, и передает MSC временный мобильный опознавательный код станции (TMSI — Temporary Mobile Station Identity).
12. MSC передает MS TMSI и информирует его о начале работы.

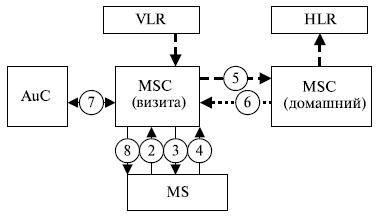
На рис. 1.12 отдельно отображен процесс изменения номеров в процессе установления входящего вызова.



**Рис. 1.12.** Принцип изменения номера

##### Регистрация в сети

При каждом включении телефона после выбора сети начинается процедура регистрации ( рис. 1.13). Рассмотрим наиболее общий случай — регистрацию не в домашней, а в чужой, так называемой гостевой, сети (будем предполагать, что услуга роуминга абоненту разрешена).



**Рис. 1.13.** Процесс регистрации

1. MS по широковещательному каналу управления (BCCH) проводит сканирование свыше 16 соседних сот, и формируется список шести лучших кандидатов на возможную передачу соединения, основанную на полученной напряженности поля сигналов.
2. MS находит канал BCCH с наиболее высоким уровнем сигнала, проводит синхронизацию, расшифровывает идентификатор BTS и передает эту информацию к BSC и MSC.
3. По запросу MSC производит запрос MS с номером IMSI.
4. MS передает IMSI абонента. IMSI начинается с кода страны "приписки" его владельца, далее следуют цифры, определяющие домашнюю сеть, а уже потом — уникальный номер конкретного подписчика. Начало IMSI соответствует коду страны и оператору (например, 250 — Россия, 99 — Билайн).
5. По номеру IMSI VLR гостевой сети определяет домашнюю сеть и запрашивает ее HLR.
6. Домашний регистр мобильного центра коммутации (MSC/HLR) передает всю необходимую информацию об абоненте в VLR, который сделал запрос, а у себя размещает ссылку на этот VLR, чтобы в случае необходимости знать, где "искать" абонента.
7. MSC совместно с VLR проводит проверку полномочий.
8. В положительном случае MSC включает MS в обслуживание.

После процедуры идентификации и взаимодействия гостевого VLR с домашним HLR запускается счетчик времени, задающий момент перерегистрации в случае отсутствия каких-либо сеансов связи. Обычно период обязательной регистрации составляет несколько часов. Перерегистрация необходима для того, чтобы сеть получила подтверждение, что телефон по-прежнему находится в зоне ее действия. Дело в том, что в режиме ожидания "трубка" только отслеживает сигналы, передаваемые сетью, но сама ничего не излучает. Процесс передачи начинается только в случае установления соединения, а также при значительных перемещениях относительно сети (ниже это будет рассмотрено подробно), — в таких случаях таймер, отсчитывающий время до следующей перерегистрации, запускается заново. Поэтому при "выпадении" телефона из сети (например, был отсоединен аккумулятор, или владелец аппарата зашел в метро, не выключив телефон) система об этом не узнает.

При первой установке абонента в сети выполняется операция закрепления международного идентификационного номера мобильной станции (IMSI — International Mobile Station Identity). Обратная закреплению процедура — открепление — позволяет сети знать, что передвижная станция недостижима, и устраняет необходимость напрасно распределять каналы и передавать широковещательные сообщения. Процедура закрепления похожа на обновление местоположения и сообщает, что мобильная станция доступна снова.

Все пользователи случайным образом разбиваются на 10 равноправных классов доступа (с номерами от 0 до 9). Абоненту присваивается класс доступа. Существует несколько специальных классов с номерами с 11 по 15 (разного рода аварийные и экстренные службы, служебный персонал сети). Информация о классе доступа хранится в SIM-карте. Особый, 10-й класс доступа позволяет совершать экстренные звонки (по номеру 112), если пользователь не принадлежит к какому-либо разрешенному классу или вообще не имеет IMSI (SIM). В случае чрезвычайных ситуаций или перегрузки сети некоторым классам может быть на время закрыт доступ в сеть.

Активация IMSI и закрепление/открепление осуществляется оператором на базе определенной соты.

##### Обновление местоположения

При подвижной связи в случае включенной мобильной станции осуществляется постоянное слежение за местоположением даже в случае отсутствия соединения. В частности, это необходимо для установления входящей связи. Включенная мобильная станция информируется о входящем вызове широковещательным сообщением, передаваемым по широковещательному каналу коротких сообщений (PCH — Paging Channel).

Один из вариантов определения местоположения — периодически сообщать о расположении объектов в каждой соте. При этом, если объект редко меняет свое местоположение (соту), такая процедура лишь понапрасну расходовала бы пропускную способность радиосети. Другой крайний случай — уведомлять систему при изменении местоположения мобильной станции широковещательным сообщением. но и это очень расточительно из-за большого количества мобильных станций, обновляющих свое местоположение. Компромиссное решение, используемое в GSM, — оповещение о местоположении при смене группы сот в зоне местоположения, приводящей к ухудшению связи. Обновляющие сообщения требуются при перемещении между областями местоположения, и передвижные станции просматриваются в сотах их текущей области.

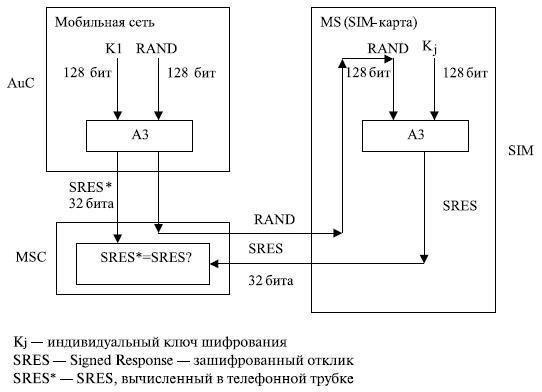
Процедуры обновления местоположения и соответствующая последующая маршрутизация используют центр коммутации мобильной связи (MSC) и два регистра местоположения: домашний регистр местоположения (HLR) и визитный регистр местоположения (VLR). Когда передвижная станция:

* переключается к другой BTS и BSC в области местоположения,
* перемещается в новую область местоположения,
* перемещается к другому оператору общедоступной телефонной сети (для наземных объектов) (PLMN — Public Land Mobile Telephone Network)

Тогда это перемещение должно регистрироваться сетью, чтобы отметить текущее местоположение. В нормальном случае сообщение обновления местоположения передают новому центру коммутации мобильной связи — MSC (визитному регистру местоположения VLR), который записывает информацию в области памяти местоположения и затем передает ее домашнему регистру местоположения — HLR абонента. Информация, передаваемая HLR, — обычно через ОКС № 7, — это адрес нового VLR, хотя это может быть номер направления. Если абонент имеет право на обслуживание в новой области местоположения, HLR передает набор абонентской информации, необходимой для управления вызовом, новому центру коммутации мобильной связи (MSC/VLR) и посылает сообщение старому MSC/VLR об отмене старой регистрации.

##### Аутентификация и защита

Так как к радиосреде имеют доступ много устройств и абонентов, требуется аутентифицировать пользователей. Эта процедура ( рис. 1.14) устанавливает подлинность и принадлежность к сети абонента и оборудования, определяет права и полномочия абонента и право доступа к сетевым ресурсам. Аутентификация проводится с помощью двух функциональных объектов: SIM-карты в мобильной станции и центра аутентификации (AuC — Authentication Center).



**Рис. 1.14.** Обеспечение аутентификации абонента и защиты информации

При регистрации AuC в домашней сети генерирует 128-битовое случайное число — RAND, пересылаемое телефону. Внутри SIM с помощью ключа Ki (ключ идентификации — так же, как и IMSI, он содержится в SIM) и алгоритма идентификации А3 вычисляется 32-битовый ответ — SRES (Signed respons) по формуле . Точно такие же вычисления проделываются одновременно и в AUC (по выбранному из HLR Ki пользователя). Если SRES, вычисленный в телефоне, совпадет со SRES, рассчитанным AuC, то процесс авторизации считается успешным и абоненту присваивается TMSI (Temporary Mobile Subscriber Identity — временный номер мобильного абонента). TMSI служит исключительно для повышения безопасности взаимодействия подписчика с сетью и может периодически меняться (в том числе при смене VLR).

То же самое случайное начальное число и абонентский ключ засекречивания также используются, чтобы вычислить ключ шифрования, который применяет алгоритм шифрования речи. Этот ключ шифрования, вместе с номером кадра TDMA, алгоритму нужен, чтобы создать последовательность на 114 битов, применяя операцию "исключающее ИЛИ" (XOR) с 114 битами пакета (два блока на 57 битов).

Другой уровень защиты выполняется в MS непосредственно для защиты оборудования от несанкционированного использования. Как упомянуто ранее, каждый терминал GSM идентифицирован уникальным международным опознавательным кодом мобильного оборудования (IMEI — Mobile Equipment Identity). Список IMEI в сети сохраняется в регистре идентификации оборудования (EIR — Equipment Identity Register), и в ответ на запрос IMEI к EIR ему возвращается одно из следующих состояний, в соответствии с тем, в каком списке находится номер абонента:

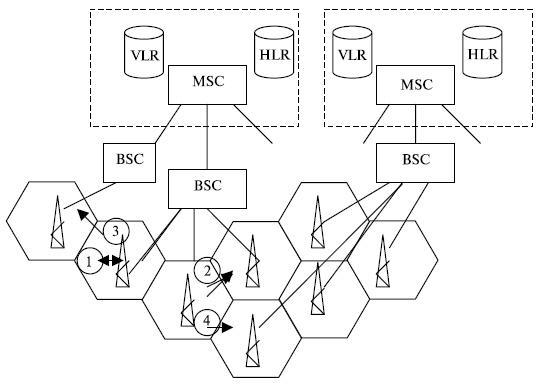
* белый список — терминалу позволяют соединиться с сетью;
* серый список — терминал находится под наблюдением сети ввиду возможных проблем;
* черный список — терминал заявлен как украденный или некорректный тип для сети GSM. Терминалу не позволяют соединиться с сетью.

##### Передача соединения (хэндовер)

В сотовой сети радиоресурсы и фиксированные линии связи в течение вызова не остаются занятыми постоянно. Хэндовер (передача соединения), или хэндофф (handoff), как его называют в Северной Америке, — это переключение каналов и линий по мере перемещения подвижного объекта по различным каналам или ячейкам сотовой сети. Обнаружение и измерение уровня радиосигналов для хэндовера составляют одну из основных функций уровня RRM (Radio Resources Management).

Хэндоверы принято разделять на четыре типа, указанных цифрами на рис. 1.15:

1. Смена каналов в пределах одной базовой станции.
2. Смена канала одной базовой станции на канал другой станции, но находящейся под управлением того же BSC.
3. Переключение каналов между базовыми станциями, контролируемыми разными BSC, но одним MSC.
4. Переключение каналов между базовыми станциями, за которые отвечают не только разные BSC, но и разные MSC.



**Рис. 1.15.** Варианты хэндовера

В общем случае проведение хэндовера — задача MSC. Но в двух первых случаях, называемых внутренними хэндоверами, чтобы снизить нагрузку на коммутатор и служебные линии связи, процесс смены каналов управляется BSC, а MSC лишь информируется о происшедшем.

Первые два типа передачи соединения называются внутренними передачами соединения и включают только один контроллер базовой станции (BSC). Чтобы сохранять способность обмена сигналами, достаточно взаимодействия базовых станций (BSC), без использования управления центра коммутации мобильной связи (MSC). После окончания передачи соединения (хэндовера) необходимо уведомить об этом событии коммутации мобильной связи (MSC).

Последние два типа передачи соединения называются внешними передачами соединения и обрабатываются центрами коммутации мобильной связи (MSC), участвующими в соединении. Важный аспект — то, что первоначальный MSC (anchor MSC — анкерный центр ), который обеспечивает доступ к сети, остается ответственным за большинство переключений.

Передачи соединения (хэндовер) могут быть инициализированы или мобильной станцией, или центром коммутации мобильной связи (MSC). MS по широковещательному каналу управления (BCCH) проводит сканирование не менее 16 соседних сот, и формируется список шести лучших кандидатов на возможную передачу соединения, основанную на полученной напряженности поля сигналов. Эта информация передается к BSC и MSC не менее одного раза в секунду для использования алгоритмом передачи соединения (хэндовера).

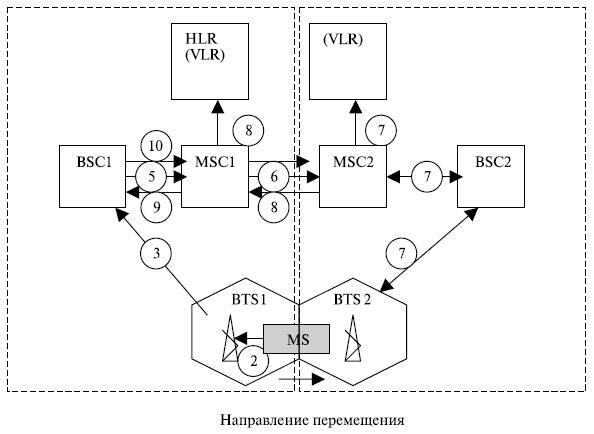
Алгоритм момента времени, когда должно быть принято решение передачи соединения (хэндовер), не определен в рекомендациях GSM. Есть два основных используемых алгоритма, оба тесно связаны с управлением мощностью. Это объясняется тем, что базовая станция (BSC) обычно не знает, является ли плохое качество сигнала следствием замирания из-за многолучевости или следствием перемещения мобильной станции к другой ячейке. Особенно часто это происходит при маленьких городских ячейках.

Алгоритм "минимально допустимая характеристика" [49] дает приоритет управлению мощностью, а не передаче соединения (хэндоверу). Когда сигнал ухудшился до некоторой заданной точки, уровень мощности мобильной станции увеличивается с помощью управления. Если дальнейшее увеличение мощности не улучшает сигнал, то начинают передачу соединения (хэндовер). Это наиболее простой и наиболее общий метод, но он создает эффект "расплывчатой границы" соты, когда мобильная станция передает сигналы, используя пиковую мощность, проходя некоторое расстояние вне границы ячейки исходной соты в другую соту.

"Метод бюджета мощности" предоставляет приоритет передаче соединения (хэндоверу). Целью является поддержание или улучшение качества сигнала при том же самом или более низком уровне мощности. В этом случае отсутствует проблема "расплывчатой границы" соты и уменьшаются межканальные помехи, но весьма усложняется алгоритм.

Рассмотрим процесс обмена сигналами, показанный на рис. 1.16, как хэндовер 4-го типа (см. рис. 1.15). Ниже приводится его описание.

1. Когда MS включена, она периодически извещает о качестве сигналов BTS1 с помощью сообщения об измерении. Эти сообщения передаются в каждом SACHH (низкоскоростной выделенный канал управления) с периодичностью 480 мсек. Сообщение об измерении содержит измерения качества сигналов соседних ячеек.
2. Если качество сигнала хорошее, то MS не предпринимает никаких действий. Когда MS достигает границы между зонами обслуживания MSC2 и MSC1, она извещает BTS1, что получает слабый сигнал.
3. BTS1 принимает решение об инициализации процесса хэндовер для того, чтобы улучшить качество обслуживания MS, и передает результаты измерений BSC1, включая измерения качества сигналов соседних ячеек BSC1.
4. BSC1 проводит анализ результатов измерения, чтобы определить зону обслуживания с лучшим качеством.
5. Если BSC1 решает запросить хэндовер, то он передает MSC1 номер используемой соты и список целевых сот с лучшими показателями, чем у используемой соты. При этом станция BTS2 включена в список целевых сот. На BSC1 включается таймер, чтобы ограничить время ожидания начала хэндовера (поступления сигнала от MSC1 о начале процесса хэндовера).
6. MSC1 передает запрос на хэндовер к MSC2. При этом из регистра MSC1 (это может быть VLR или HLR) передаются данные для маршрутизации и аутентификации. На MSC1 включается таймер, чтобы ограничить время ожидания начала хэндовера в зоне обслуживания MSC2 (время ответа от BCS2).
7. На MSC2 запрос на передачу соединения обрабатывается как новый исходящий вызов и выбирается канал для нового вызова. Новые данные записываются в VLR MSC2. VLR MSC2 обеспечивает присвоение номера "блуждающей" подвижной станции (MSRN — Mobile Station Roaming Number). Процедурами установления подлинности во время обработки вызова управляет VLR MSC2.
8. Передача подтверждения запроса хэндовера от MSC2 (начало хэндовера) к MSC1. На MSC1 отключается таймер, ограничивающий время ожидания начала хэндовера (см. п. 7), так как получена команда о начале хэндовера. Если MSC1 был центром визита, то данные на VLR MSC1 стираются. Если он был домашним центром, то текущий адрес VLR абонента, содержащийся в HLR, также обновляется.
9. MSC1 передает сообщение BSC1, что соединение закончено.
10. BSС1 освобождает канал и информирует MSC1, что разъединение закончено.
11. MSC1 освобождает оборудование и передает MSC2 сигнал окончания процедуры.



**Рис. 1.16.** Обмен сигналами при хэндовере

##### Роуминг

Роуминг — одна из самых важных функций сотовой связи. Необходимость в роуминге возникает каждый раз, когда абонент изменяет свое местоположение и перемещается в сеть, принадлежащую другому оператору. Роуминг бывает локальный (переезд внутри города или в пригород), национальный (в другой город или область) и международный (переезд в другую страну).

При перемещении абонента в другую сеть ее центр коммутации **мобильной связи** (MSC/VLR) запрашивает информацию в первоначальной сети (MSC/HLR) и при наличии подтверждения полномочий абонента регистрирует его. Данные о местоположении абонента постоянно обновляются в центре коммутации первоначальной сети (MSC/HLR), и все поступающие туда вызовы автоматически переадресовываются в ту сеть, где в данный момент находится абонент.

По способу регистрации различают следующие виды роуминга:

* автоматический, т. е. с возможностью провести процесс хэндовера;
* полуавтоматический, когда предварительно следует оповестить оператора о намерении посетить соответствующий регион;
* ручной, при котором абоненту вручается радиотелефон, включенный в сеть визита.

Для обеспечения роуминга необходимо выполнение следующих условий:

* наличие в требуемых регионах сотовых систем стандарта, совместимого со стандартом компании, у которой был приобретен радиотелефон;
* наличие соответствующих организационных и экономических соглашений о роуминговом обслуживании абонентов;
* наличие каналов связи между системами, обеспечивающих передачу звуковой, сигнальной и другой информации для роуминговых абонентов.

При организации роуминга недостаточно провести только технические мероприятия по соединению различных сетей сотовой связи. Очень важно еще решить проблему взаиморасчетов между операторами этих сетей.

Кроме того, для организации передачи сигнальных сообщений при автоматическом роуминге нужно создать соответствующие сигнальные каналы и программное обеспечение. Это требует определенных затрат. Поэтому между областями обслуживания различных операторов должна быть большая потребность в обслуживании роуминговой связи — больше, чем просто трафик от "случайно заехавших" абонентов.

**Лекция 9. GPRS и EDGE**

**Что такое GPRS.**

Одним из существенных недостатков сетей сотовой связи стандарта GSM на сегодняшний день является низкая скорость передачи данных (максимум 9.6 кбит/с). Да и сама организация этого процесса далека от совершенства - для передачи данных абоненту выделяется один голосовой канал, а биллинг осуществляется исходя из времени соединения (причем по тарифам, мало отличающимся от речевых).

Для высокоскоростной передачи данных посредством существующих GSM-сетей и была разработана GPRS (General Packet Radio Service - услуга пакетной передачи данных по радиоканалу). Необходимо отметить, что кроме повышения скорости (максимум составляет 171.2 кбит/с, но об этом чуть ниже), новая система предполагает иную схему оплаты услуги передачи данных - при использовании GPRS расчеты будут производиться пропорционально объему переданной информации, а не времени, проведенному online. К тому же, введение GPRS будет способствовать более бережливому и рациональному распределению радиочастотного ресурса: особо не вдаваясь в технические тонкости можно сказать, что "пакеты" данных предполагается передавать одновременно по многим каналам (именно в одновременном использовании нескольких каналов и заключается выигрыш в скорости) в паузах между передачей речи. И только в паузах - голосовой трафик имеет безусловный приоритет перед данными, так что скорость передачи информации определяется не только возможностями сетевого и абонентского оборудования, но и загрузкой сети. Подчеркну, что в GPRS ни один канал не занимается под передачу данных целиком - и это основное качественное отличие новой технологии от используемых ныне.

Разумеется, разработчики GPRS приложили все усилия для того, чтобы установка новой системы "поверх" существующих GSM-сетей оказалась как можно менее обременительной (и разорительной, что немаловажно) для операторов. Давайте рассмотрим подробнее, какие новые блоки и связи появляются в общей архитектуре системы сотовой связи стандарта GSM с внедрением GPRS, а потом обсудим пользовательское оборудование, способное работать с высокоскоростной пакетной передачей данных.

**GPRS изнутри.**

Доработку GSM-сети для предоставления услуг высокоскоростной передачи данных GPRS можно условно разделить на две формы - программную и аппаратную. Если говорить о программном обеспечении, то оно нуждается в замене или обновлении практически всюду - начиная с реестров HLR-VLR и заканчивая базовыми станциями BTS. В частности, вводится режим многопользовательского доступа к временным кадрам каналов GSM, а в HLR, например, появляется новый параметр Mobile Station Multislot Capability (количество каналов, с которыми одновременно может работать мобильный телефон абонента, но об этом ниже).

Ядро системы GPRS (GPRS Core Network) состоит из двух основных блоков - SGSN (Serving GPRS Support Node - узел поддержки GPRS) и GGPRS (Gateway GPRS Support Node - шлюзовой узел GPRS). Остановимся на их функциях более подробно.

SGSN является, грубо говоря, мозгом рассматриваемой системы. В некотором роде SGSN можно назвать аналогом MSC - коммутатора сети GSM. SGSN контролирует доставку пакетов данных пользователям, взаимодействует с реестром собственных абонентов сети HLR, проверяя, разрешены ли запрашиваемые пользователями услуги, ведет мониторинг находящихся online пользователей, организует регистрацию абонентов вновь "проявившихся" в зоне действия сети и т.п. Так же как и MSC, SGSN, в системе может быть и не один - в этом случае каждый узел отвечает за свой участок сети. Например, SGSN производства компании Motorola имеет следующие характеристики: каждый узел поддерживает передачу до 2000 пакетов в секунду, одновременно контролирует до 10000 находящихся online пользователей. Всего же в системе может быть до 18 SGSN Motorola.

Предназначение GGSN можно понять из его названия - грубо говоря, это шлюз между сотовой сетью (вернее, ее частью для передачи данных GPRS) и внешними информационными магистралями (Internet, корпоративными интранет-сетями, другими GPRS системами и так далее). Основной задачей GGSN, таким образом, является роутинг (маршрутизация) данных, идущих от и к абоненту через SGSN. Вторичными функциями GGSN является адресация данных, динамическая выдача IP-адресов, а также отслеживание информации о внешних сетях и собственных абонентах (в том числе тарификация услуг).

Замечу, что в GPRS-систему заложена хорошая масштабируемость - при появлении новых абонентов оператор может увеличивать число SGSN, а при эскалации суммарного трафика - добавлять в систему новые GGSN. Внутри ядра GPRS-системы (между SGSN и GGSN) данные передаются с помощью специального туннельного протокола GTP (GPRS Tunneling Protocol).

Еще одной составной частью системы GPRS является PCU (Packet Control Unit - устройство контроля пакетной передачи). PCU стыкуется с контроллером базовых станций BSC и отвечает за направление трафика данных непосредственно от BSC к SGSN.

В перспективе (при ориентации системы на мобильный Интернет) возможно добавление специального узла - IGSN (Internet GPRS Support Node - узел поддержки Интернет).

За управление и контроль GPRS-системы отвечает OMC-R/G (Operation and Maintenance Center - Radio/GSN - центр управления и обслуживания радио/узла GPRS: на рис.1 не показан). Это, так сказать, интерфейс между системой и обслуживающим ее персоналом.

Прежде чем приступить к работе с GPRS, мобильная станция, так же как и в обычном случае передачи голоса, должна зарегистрироваться в системе. Как уже было сказано, регистрацией (а, точнее, "прикреплением" (attachment) к сети) пользователей занимается SGSN. В случае успешного прохождения всех процедур (проверки доступности запрашиваемой услуги и копирования необходимых данных о пользователе из HLR в SGSN) абоненту выдается P-TMSI (Packet Temporary Mobile Subscriber Identity - временный номер мобильного абонента для пакетной передачи данных), аналогичный TMSI, который назначается мобильному телефону для передачи голоса (кстати, если абонентский терминал относится к классу А (см. ниже), то ему при регистрации выделяется как TMSI, так и P-TMSI).

Для быстрой маршрутизации информации к мобильному абоненту GPRS-система нуждается в данных о его месторасположении относительно сети, причем с большей точностью, нежели в случае передачи голосового трафика (напомню, HLR и VLR хранят номер Location Area (LA), в которой находится абонент. Но представьте себе, как возрастет служебный трафик в сотовой сети и расход энергии мобильным аппаратом, если телефон будет информировать систему каждый раз при переходе от одной соты к другой! Чтобы найти разумный компромисс между объемом сигнального трафика в сети GPRS и необходимостью знать с высокой точностью местонахождение абонента принято деление терминалов на три класса:

* IDLE (неработающий). Телефон отключен или находится вне зоны действия сети. Очевидно, что система не отслеживает перемещение подобных абонентов.
* STANDBY (режим ожидания). Аппарат зарегистрирован (прикреплен) в GPRS-системе, но уже долгое время (определяемое специальным таймером) не работает с передачей данных. Местоположение STANDBY-абонентов известно с точностью до RA (Routing Area - область маршрутизации). RA мельче, чем LA (каждая LA разбивается на несколько RA, но, тем не менее, RA крупнее, чем сота, и состоит из нескольких элементарных ячеек).
* READY (готовность). Абонентский терминал зарегистрирован в системе и находится в активной работе. Координаты телефонов, находящихся в режиме READY, известны системе (а, точнее, SGSN) с точностью до соты.

Согласно этой идеологии, терминалы, находящиеся в STANDBY-режиме, при переходе из одного RA в другой посылают SGSN специальный сигнал о смене области маршрутизации (routing area update request). Если новая и старая RA контролируется одним SGSN, то смена RA приводит лишь к корректировке записи в SGSN. Если же абонент переходит в зону действия нового SGSN, то новый SGSN запрашивает у старого информацию о пользователе, а MSC, VLR, HLR и вовлеченные в работу GGSN ставятся в известность о смене SGSN. Когда телефон, работающий с GPRS-системой, перемещается в другую LA, то SGSN отправляет соответствующему VLR сообщение о необходимости смены записи о местонахождении абонента.

Интересно обстоят дела с маршрутизацией данных в случае роуминга GPRS-абонента. При этом возможны два варианта, или, правильней сказать, сценария. SGSN в обоих случаях используется гостевой (VSGSN - Visited SGSN), а вот GGSN может использоваться либо гостевой (VGGSN - Visited GGSN), либо домашний (HGGSN - Home GGSN). В последнем случае между домашним и гостевым операторами должна существовать GPRS-магистраль (InterPLMN GPRS BackBone - GPRS-линия между разными мобильными сетями) для передачи трафика между HGGSN и мобильным абонентом. Кроме того, появляется необходимость в BG (Border Gateway - граничный шлюз) с обеих сторон с целью обеспечения защиты сетей от атак извне.

Следует отметить такой важный параметр, как QoS (Quality of Service - качество сервиса). Очевидно, что видеоконференция в режиме реального времени и отправка сообщения электронной почты предъявляют разные требования, например, к задержкам на пути пакетов данных. Поэтому в GPRS существует несколько классов QoS, подразделяющихся по следующим признакам:

* необходимому приоритету (существует высокий, средний и низкий приоритет данных);
* надежности (разделение на три класса по количеству возможных ошибок разного рода, потерянных пакетов и т.п.);
* задержкам (задержки информации вне GPRS-сети в расчет не принимаются);
* количественным характеристикам (пиковое и среднее значение скорости);

Класс QoS выбирается индивидуально для каждой новой сессии передачи данных.

Кроме QoS, в характеристику сессии передачи данных входит тип протокола (PDP type - Packet Data Protocol type); PDP-адрес, выданный мобильной станции (выдача адресов бывает как статической, так и динамической); а также адрес GGSN, с которым идет работа. "Профиль" сессии (в англоязычной литературе принято обозначение "PDP context") записывается в телефон, а также в обслуживающие его SGSN и GGSN. Одновременно может поддерживаться несколько профилей передачи данных для каждого пользователя.

Вообще говоря, пакетная передача данных предусматривает два режима "соединений":

* PTP (Point-To-Point - точка-точка);
* PTM (Point-To-Multipoint - точка-многоточие).
* Широковещательный режим РТМ в свою очередь подразделяется на два класса:
* PTM-M (PTM-Multicast) - передача необходимой информации всем пользователям, находящимся в определенной географической зоне;
* PTM-G (PTM-Group Call) - данные направляются определенной группе пользователей.

Поддержка режима "многоточечной" передачи информации PTM ожидается в будущих спецификациях GPRS.

* 1. ***Принцип работы***

При использовании GPRS информация собирается в пакеты и передаётся через неиспользуемые в данный момент голосовые каналы. Такая технология предполагает более эффективное использование ресурсов сети GSM. При этом, что именно является приоритетом передачи — голосовой трафик или передача данных — выбирается оператором связи. Федеральная тройка в России использует безусловный приоритет голосового трафика перед данными, поэтому скорость передачи зависит не только от возможностей оборудования, но и от загрузки сети. Возможность использования сразу нескольких каналов обеспечивает достаточно высокие скорости передачи данных, теоретический максимум при всех занятых таймслотах TDMA составляет 171,2 кбит/c. Существуют различные классы GPRS, различающиеся скоростью передачи данных и возможностью совмещения передачи данных с одновременным голосовым вызовом.

Передача данных разделяется по направлениям «вниз» (downlink; DL) — от сети к абоненту, и «вверх» (uplink, UL) — от абонента к сети. Мобильные терминалы разделяются на классы по количеству одновременно используемых таймслотов для передачи и приёма данных. Современные телефоны (июнь 2006) поддерживают до 4-х таймслотов одновременно для приёма по линии «вниз» (то есть могут принимать 85 кбит/с по кодовой схеме CS-4), и до 2-х для передачи по линии «вверх» (class 10 или 4+2 всего 5). Новейшие телефоны (февраль 2009) поддерживают class 12 (или 4+4, всего 5).

Абоненту, подключенному к GPRS, предоставляется виртуальный канал, который на время передачи пакета становится реальным, а в остальное время используется для передачи пакетов других пользователей. Поскольку один канал могут использовать несколько абонентов, возможно возникновение очереди на передачу пакетов, и, как следствие, задержка связи. Например, современная версия программного обеспечения контроллеров базовых станций допускает одновременное использование одного таймслота шестнадцатью абонентами в разное время и до 5 (из 8) таймслотов на частоте, итого - до 80 абонентов, пользующихся GPRS на одном канале связи (средняя максимальная скорость при этом 21,4\*5/80 = 1,3 кбит/с на абонента). Другой крайний случай - пакетирование таймслотов в один непрерывный с вытеснением голосовых абонентов на другие частоты (при наличии таковых и с учётом приоритета). При этом телефон, работающий в режиме GPRS, принимает все пакеты на одной частоте и не тратит времени на переключения. В этом случае скорость передачи данных достигает максимально возможной, как и описано выше, 4+2 таймслота (class 10) или 4+4 (class 12).

Технология GPRS использует GMSK-модуляцию. В зависимости от качества радиосигнала, данные, пересылаемые по радиоэфиру, кодируются по одной из 4-х кодовых схем (CS1—CS4). Каждая кодовая схема характеризуется избыточностью кодирования и помехоустойчивостью, и выбирается автоматически в зависимости от качества радиосигнала. По той же схеме и используя то же самое оборудование, работает и технология EDGE. Но внутри таймслота EDGE используется другая, более плотная, упаковка информации (модуляция 8PSK).

**GPRS снаружи - абонентские устройства.**

Поговорим теперь о клиентском оборудовании GPRS. К сожалению или к счастью, но для работы с системой пакетной передачи данных необходимо иметь специальный телефон, совместимый с GPRS. Говоря более строго, GPRS-терминалы подразделяются на три класса:

* устройства **класса А** способны одновременно работать как с передачей голоса, так и с передачей данных (они, говоря техническим языком, обладают возможностью функционировать как в режиме коммутации каналов (circuit switched), так и в режиме коммутации пакетов (packet switched). Подчеркну - речь идет об одновременной работе в разных режимах);
* устройства **класса В** могут осуществлять либо передачу голоса, либо передачу данных, но не одновременно;
* устройства **класса С** поддерживают только передачу данных и не могут быть использованы для голосовой связи. Как правило, это разного рода компьютерные платы для обеспечения беспроводного доступа к данным.

Следует заметить, что максимальная скорость передачи данных определяется, в первую очередь, количеством каналов, с которыми одновременно может работать абонентский терминал. Один канал обеспечивает передачу данных со скоростью до 13.4 кбит/с.

* 1. ***Интеграция с Интернетом***

GPRS по принципу работы аналогична Интернету: данные разбиваются на пакеты и отправляются получателю (необязательно одним и тем же маршрутом), где происходит их сборка. При установлении сессии каждому устройству присваивается уникальный адрес, что по сути превращает его в сервер. Протокол GPRS прозрачен для TCP/IP, поэтому интеграция GPRS с Интернетом незаметна конечному пользователю. Пакеты могут иметь формат IP или X.25, при этом не имеет значения, какие протоколы используются поверх IP, поэтому есть возможность использования любых стандартных протоколов транспортного и прикладного уровней, применяемых в Интернете (TCP, UDP, HTTP, HTTPS, SSL, POP3, XMPP и др.). Также при использовании GPRS мобильный телефон выступает как клиент внешней сети, и ему присваивается IP-адрес (постоянный или динамический).

EDGE (EGPRS) (англ. Enhanced Data rates for GSM Evolution) — цифровая технология беспроводной передачи данных 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. EDGE был впервые представлен в 2003 году в Северной Америке.

Система EDGE планировалась для того, чтобы операторы GSM могли ее применить в существующей сети в процессе перехода к UMTS. При этом они могли использовать в своих интересах спектр IMT-2000. Поскольку UMTS может выполнять хэндовер к GSM, обе эти технологии были бы совместимы, и большое количество терминалов, проданных в Европе, были бы способны работать через обе системы.

Все изменилось, когда EDGE был создан UWCC (Universal Wireless Communications Consortium — Консорциум универсальной беспроводной связи), совет, представляющий американскую промышленность выпускающую TDMA. Работая с GSM-Ассоциацией, они разработали способ модернизации D-AMPS к EDGE. Объяснение этого факта простое: DAMPS выполнила свою задачу, так что операторам надо было строить новые сети 3G. И CDMA2000, и WCDMA были рассчитаны на построение этих новых сетей, но проблема была в широких каналах. Любая система радиосвязи, чтобы работать, нуждается по крайней мере в одном канале, а для оператора это необходимость новой лицензии.

Новый радиоинтерфейс EDGE, созданный на основе стандартов GSM, обеспечивает плавный переход к системам радиосвязи 3-го поколения, позволяя увеличить скорость передачи данных до 384 Кбит/с. Что же касается более высоких скоростей передачи (от 2048 Кбит/с), которые определены в IMT-2000 для новых поколений пико- и микросотовых сетей, то их предполагается реализовать во второй фазе спецификаций.

Ширина канала EDGE — 200 кГц, такая же, как у GSM. Даже условия повторного использования каналов одинаковы. В 2000 г. ITU принял EDGE как режим IMT-2000 и стандартизировал его как UWC-136. В спецификациях EDGE заложены принципиально новые по сравнению с GSM возможности. В первую очередь это автоматическое распознавание типа модуляции, применяемого в радиолинии, с автоматическим переходом в требуемый режим. Усовершенствованный метод модуляции позволяет абонентской радиостанции автоматически адаптироваться к качеству канала радиосвязи, причем самые высокие скорости передачи обеспечиваются, безусловно, в наиболее благоприятных условиях распространения радиоволн (например, вблизи базовых станций). Втаблице приведены сравнительные характеристики систем EDGE и WCDMA.

|  |  |  |
| --- | --- | --- |
| Показатель | EDGE | WCDMA |
| Скорость передачи в условиях высокой мобильности в локальных зонах покрытия, Кбит/c | 128 | 384 |
| Скорость передачи в условиях низкой мобильности в широких зонах покрытия, Кбит/c | 384 | 2048 |
| Используемые диапазоны частот, МГц | GSM (450, 900, 1800) и PCS (1900) | 1920–1980, 2110–2170 |
| Ширина полосы канала, МГц | 0,2 | 5 |
| Метод доступа/модуляции | TDMA/8PSK | DS-CDMA/QPSK |
| Мощность передатчика мобильного терминала (передача речи), Вт | 1 (макс.) | 0,125 |

Технология EDGE предусматривает организацию двух служб: усовершенствованной службы пакетной передачи (EGPRS — Enhanced GPRS) и усовершенствованной службы коммутации каналов (ECSD — Enhanced Circuit Switched Data). Она унаследовала почти все свои главные особенности от GSM и GPRS, включая структуру кадра TDMA с восемью слотами длиною слота 0,577 мс. Разница заключается в схеме модуляции. Вместо двоичной GMSK (Gaussian Minimum Shift Keying — гауссовская манипуляция с минимальным сдвигом), применяется 8-PSK, такая же, как в HDR. Это сразу утраивает пропускную способность по сравнению с GSM.

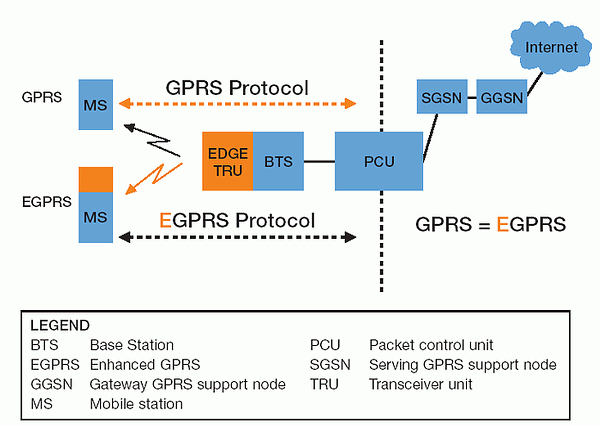
## EDGE — что это такое и с чем её едят?

Технология EDGE может внедряться двумя разными способами: как расширение GPRS, в этом случае ее следует называть EGPRS (enhanced GPRS) или как расширение CSD (ECSD). Учитывая, что GPRS распространена намного шире, чем HSCSD, остановимся на рассмотрении EGPRS.

1. EDGE не является новым стандартом сотовой связи.

Однако, EDGE подразумевает дополнительный физический уровень, который может быть использован для увеличения пропускной способности сервисов GPRS или HSCSD. При этом, сами сервисы предоставляются точно так же, как и раньше. Теоретически, сервис GPRS способен обеспечивать пропускную спосность до 160 Кбит/с (на физическом уровне, **на практике же поддерживающие GPRS Class 10 или 4+1/3+2 аппараты обеспечивают лишь до 38-42 Кбит/с** и то, если позволяет загруженность сети сотовой связи), а EGPRS — до 384-473,6 Кбит/с. Для этого необходимо использование новой модуляционной схемы, новых методов кодирования каналов и коррекции ошибок.

2. EDGE, по сути, является «надстройкой» (вернее, подстройкой, если считать, что физический уровень находится ниже остальных) к GPRS и не может существовать отдельно от GPRS. EDGE, как уже было сказано выше, подразумевает использование иных модуляционных и кодовых схем, сохраняя совместимость с CSD-сервисом голосовой связи.



*Измененные узлы показаны желтым цветом.*

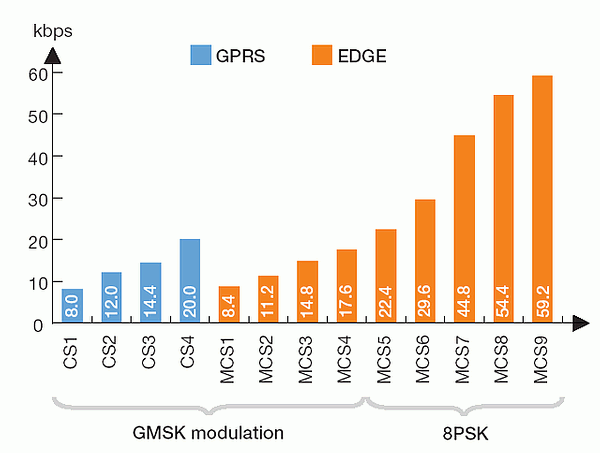
Таким образом, с точки зрения клиентского терминала, с внедрением EDGE не должно измениться ничего. Однако, инфраструктура базовой станции претерпит некоторые изменения (см. рис. 1), хотя и не такие уж серьезные. Помимо увеличения пропускной способности для передачи данных, внедрение EDGE увеличивает емкость сети сотовой связи: в один и тот же тайм-слот можно теперь «упаковать» большее количество пользователей, соответственно, можно надеяться не получать сообщение «сеть занята» в самые неподходящие моменты.

Таблица 1 иллюстрирует разные технические характеристики EDGE и GPRS. Хотя и в EDGE, и в GPRS в единицу времени отправляется одинаковой число символов, благодаря использованию другой модуляционной схемы, число бит данных в EDGE втрое больше. Сразу оговоримся здесь, что приведенные в таблице значения пропускной способности и скорости передачи данных отличаются друг от друга из-за того, что в первой также учитываются заголовки пакетов, пользователю ненужные. Ну, а максимальная скорость передачи данных в 384 Кбит/с (требуемая для соответствия спецификациям IMT-2000) получается в том случае, если используется восемь тайм-слотов, то есть, на каждый тайм-слот приходится по 48 Кбит/с.

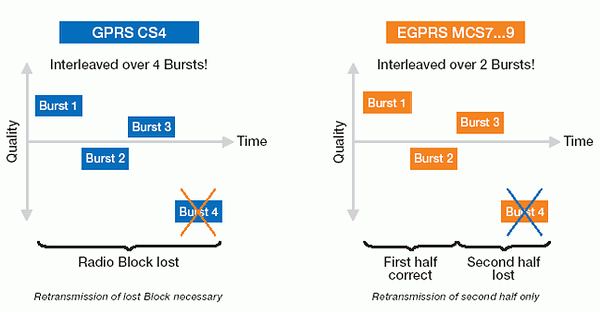
|  |  |  |
| --- | --- | --- |
| **Таблица 1. Сравнительные характеристики EDGE и GPRS** |  |  |
|  | GPRS | EDGE |
| **Модуляционная схема** | GMSK | 8-PSK/GMSK |
| **Скорость передачи символов** | 270 тыс. в секунду | 270 тыс. в секунду |
| **Пропускная способность** | 270 Кбит/с | 810 Кбит/с |
| **Пропускная способность на тайм-слот** | 22,8 Кбит/с | 69,2 Кбит/с |
| **Скорость передачи данных на тайм-слот** | 20 Кбит/с (CS4) | 59,2 Кбит/с (MCS9) |
| **Скорость передачи данных с использованием 8 тайм-слотов** | 160 (182,4) Кбит/с | 473,6 (553,6) Кбит/с/s |

* + 1. **Кодирование**

В GPRS возможно применение четырех разных схем кодирования: CS1, CS2, CS3 и CS4, в каждой из которых используется свой алгоритм коррекции ошибок. Для EGPRS разработано девять схем кодирования, MCS1..MCS9, соответственно, назначение которых также в обеспечении коррекции ошибок. Причем в «младших» MSC1..MSC4 используется модуляционная схема GMSK, в «старших» MSC5..MSC9 — модуляционная схема 8PSK. На рисунке 3 представлена зависимость скорости передачи данных от использования разных модуляционных схем вкупе с разными схемами кодирования (скорость передачи данных меняется в зависимости от того, как много требуемой для работы алгоритмов коррекции ошибок избыточной информации закладывается в каждый кодируемый пакет). Нетрудно догадаться, что чем хуже условия приема (отношение сигнал/шум), тем больше приходится закладывать избыточной информации в каждый пакет, а значит, тем меньше скорость передачи данных. Небольшое отличие в скорости передачи данных, наблюдаемое между CS1 и MCS1, CS2 и MCS2, и т. д., связано с разницей в величине заголовков пакетов.

  
*Разные кодовые схемы в GPRS и EDGE.*

Впрочем, если соотношение сигнал/шум невелико, не все потеряно: в старших модуляционно-кодовых схемах EGPRS MCS7, MCS8, MCS9 предусмотрена процедура «наложения»: так как стандарт способен отправлять группы пакетов на разных несущих (внутри частотного диапазона), для каждой из которых условия (и прежде всего — «зашумленность») могут быть разными, в этом случае повторной передачи всего блока можно избежать, если знать, в какой группе произошел сбой и повторно транслировать именно эту группу. В отличие от старшей кодовой схемы GPRS CS4, где не используется аналогичный алгоритм коррекции ошибок, в EGPRS MCS7, MCS8, MCS9 разные блоки данных «накладываются» друг на друга, поэтому при сбое в одной из групп (как показано на рисунке), повторной пересылке подлежит лишь половина пакетов.

  
*Рисунок 4. Использование наложения групп пакетов в EDGE.*

* + 1. **Обработка пакетов**

Если по каким-то причинам пакет, отправленный с использованием «старших» схем кодирования, не был корректно принят, EGPRS позволяет его ретранслировать заново с использованием «пониженной» кодировочной схемы. В GPRS такой возможности, названной «ресегментацией» (resegmentation), предусмотрено не было: некорректно принятый пакет отправляется вновь по той же модуляционно-кодировочной схеме, что и в предыдущий раз.

* + - 1. **Окно адресации (addressing window)**

Прежде чем последовательность кодированных (то есть, в которые закодированы «слова», состоящие из нескольких бит) пакетов (фрейм) может быть передана по радиочастотному интерфейсу, передатчик присваивает пакетам идентификационный номер, включенный в заголовок каждого пакета. Номера пакетов в GPRS составляют от 1 до 128. После того, как последовательность пакетов (например, 10 штук) отправлена адресату, передатчик ждет от приемника подтверждения того, что они были приняты. В отчете, который приемник отправляет обратно передатчику, содержатся номера пакетов, которые были успешно декодированы, и которые получатель декодировать не смог. Важный нюанс: номера пакетов принимают значения от 1 до 128, а ширина адресного окна — всего 64, вследствие чего вновь передаваемый пакет может получить такой же номер, как в предыдущем фрейме. В этом случае протокол вынужден повторно отправлять весь текущий фрейм, что отрицательно сказывается на скорости передачи данных в целом. Для снижения риска возникновения такой ситуации в EGPRS номер пакета может принимать значения от 1 до 2048, а адресное окно увеличено до 1024.

* + - 1. **Точность измерения**

Для обеспечения корректного функционирования технологии GPRS в среде GSM приходится постоянно измерять радиоусловия: уровень сигнал/шум в канале, частоту появления ошибок и т. п. Эти измерения никак не сказываются на качестве голосовой связи, где достаточно постоянно использовать одну и ту же кодировочную схему. При передаче данных в GPRS измерение радиоусловий возможно лишь в «паузах» — дважды за период 240 мс. Для того, чтобы не ждать каждые 120 мс, EGPRS определяет такой параметр, как вероятность возникновения ошибки на бит (BEP, bit error probability), в каждом фрейме. На величину BEP влияет как отношение сигнал/шум, так и временная дисперсия сигнала и скорость перемещения терминала. Изменение BEP от фрейма к фрейму позволяет оценить скорость терминала и «дрожание» частоты, но для более точной оценки используется среднее значение вероятности ошибки на бит на каждые четыре фрейма и его выборочное стандартное отклонение. Благодаря этому, EGPRS быстрее реагирует на изменения условий: увеличивает скорость передачи данных при снижении BEP и наоборот.

* + - 1. **Контроль за скоростью соединения в EGPRS**

В EGPRS используется комбинация двух подходов: подстройки скорости соединения и инкрементной избыточности. Подстройка скорости соединения, измеряемой либо мобильным терминалом по количеству принимаемых в единицу времени данных, либо базовой станцией по количеству, соответственно, передаваемых данных, позволяет выбрать оптимальную модуляционно-кодовую схему для последующих объемов данных. Обычно, использование новой модуляционно-кодовой схемы может быть назначено при передаче нового блока (по четыре группы) данных.

Инкрементная избыточность изначально применяется для самой старшей модуляционно-кодовой схемы, MCS9, с незначительным вниманием к коррекции ошибок и без учета условий радиосвязи. Если информация декодируется адресатом некорректно, по каналу связи передаются не сами данные, а некий контрольный код, который «добавляется» (используется для преобразования) к уже загруженным данным до тех пор, пока данные не будут декодированы успешно. Каждый такой «инкрементный кусочек» дополнительного кода увеличивает вероятность успешной расшифровки переданных данных — в этом и заключается избыточность. Главным преимуществом этого подхода является то, что здесь нет необходимости следить за качеством радиосвязи, поэтому инкрементная избыточность является обязательной в стандарте EGPRS для мобильных терминалов.

Как уже было сказано выше, главное различие между GPRS и EGPRS — в использовании иной модуляционной схемы на физическом уровне. Поэтому для поддержки EGPRS достаточно установки на базовой станции поддерживающего новые модуляционные схемы трансивера и программного обеспечения для обработки пакетов. Для обеспечения совместимости с не поддерживающими EDGE мобильными телефонами, в стандарте прописано следующее:

* Поддерживающие и не поддерживающие EDGE мобильные терминалы должны быть способны использовать один и тот же тайм-слот
* Поддерживающие и не поддерживающие EDGE трансиверы должны использовать один и тот же частотный диапазон
* Возможна частичная поддержка EDGE

Для облегчения процесса внедрения на рынок новых мобильных телефонов было решено подразделить EDGE-совместимые терминалы на два класса:

* Поддерживающие модуляционную схему 8PSK только в приемном потоке данных (downlink) и
* Поддерживающие 8PSK как в приемном, так и в передающем (uplink) потоке данных

Внедрение EGPRS, как уже говорилось выше, позволяет достичь пропускной способности, примерно втрое больше, чем в технологии GPRS. При этом используется в точности такие же профили QoS (quality of service, качество сервиса), как в GPRS, но с учетом увеличившейся пропускной способности. Помимо необходимости установки трансивера на базовой станции, для поддержки EGPRS требуется обновление программного обеспечения, которое должно будет обрабатывать измененный протокол передачи пакетов.

Следующим эволюционным шагом на пути систем сотовой связи GSM/EDGE к «полноценным» сетям третьего поколения будет дальнейшее улучшение сервисов пересылки пакетов (данных) для обеспечения их совместимости с UMTS/UTRAN (UMTS terrestrial radio access network). Эти улучшения в настоящее время проходят рассмотрениеи, скорее всего, будут включены в будущий вариант спецификаций 3GPP (3G Partnership Project). Главное отличие GERAN от внедряемой в настоящий момент технологии EDGE будет поддержка QoS для интерактивных, фоновых, потоковых и переговорных классов. Поддержка этих QoS-классов уже есть в UMTS, благодаря чему в сетях UMTS (скажем, W-CDMA 2100 или 1900 МГц) наличествует возможность, например, видеосвязи. Кроме этого, в будущем поколении EDGE планируется обеспечить одновременную параллельную обработку потоков данных с разным приоритетом QoS.

# Лекция 13. Система сотовой подвижной связи CDMA

CDMA (Code Division Multiple Access) - технологии связи с цифровыми шумоподобными сигналами на основе метода многостанционного доступа с кодовым разделением каналов

Замечательное свойство цифровой связи с шумоподобными сигналами - защищенность канала связи от перехвата, помех и подслушивания. Именно поэтому данная технология была изначально разработана и использовалась для вооруженных сил США. В 90-е годы компания Qualcom на основе этой технологии создала стандарт IS-95 (CDMA one, 2G) и передала его для коммерческого использования. На основе CDMA one были разработаны стандарты CDMA 2000, также принципам CDMA следует технология UMTS, которая взята за основу сетей третьего поколения.

### Общая характеристика и принципы функционирования

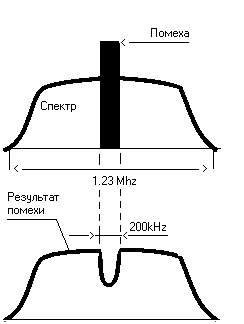
Принцип работы систем сотовой связи (ССС) с кодовым разделением каналов можно пояснить на следующем примере.

Предположим, что вы сидите в ресторане. За каждым столиком находится два человека. Одна пара разговаривает между собой на английском языке, другая на русском, третья на немецком и т.д. Получается так, что в ресторане все разговаривают в одно и то же время на одном диапазоне частот (речь от 3 кГц до 20 кГц), при этом вы, разговаривая со своим оппонентом, понимаете только его, но слышите всех.

Так же и в стандарте CDMA передаваемая в эфире информация от базовой станции к мобильной или наоборот попадает ко всем абонентам сети, но каждый абонент понимает только ту информацию, которая предназначена для него, т.е. русский понимает только русского, немец только немца, а остальная информация отсеивается. Язык общения в данный момент является кодом. В CDMA это организовано за счет применения кодирования передаваемых данных, если точнее, то за это отвечает блок умножения на функцию Уолша.

В отличие от стандарта GSM, который использует TDMA (Time Division Multiple Access - многостанционный доступ с кодовым разделением канала, т.е. несколько абонентом могут разговаривать на одной и той же частоте, как и в CDMA, но в отличие от CDMA, в разное время), стандарт IS-95 диапазон частот использует более экономично.

CDMA называют широкополосной системой и сигналы идущие в эфире шумоподобными. Широкополосная - потому, что занимает широкую полосу частот. Шумоподобные сигналы - потому, что когда в эфире на одной частоте, в одно и то же время работают несколько абонентов, сигналы накладываются друг на друга (можно представить шум в ресторане, когда все одновременно говорят). Помехоустойчивая - потому, что при возникновении в широкой полосе частот(1,23 Мгц) сигнала-помехи, узкого диапазона (<150кГц), сигнал примется почти неискаженный. За счет помехоустойчивого кодирования потерянные данные система восстановит, см. рис 1, где показан полезный сигнал и помеха (СЗС - селективная помеха).

А в стандарте GSM такое не получится. Из-за того, что GSM изначально сам узкополосный. Ширина полосы, которая используется, равна 200 кГц. 

CDMA One – это первый стандарт мобильной связи, который придал толчок повсеместному использованию сотовой связи и нашел широкое распространение в Северной Америке. CDMA One – это только брендовое имя стандарта, часто упоминаемого как IS-95. Первые спецификации стандарта IS-95 выпускались под аббревиатурой IS-95A, а более поздние, усовершенствованные релизы опубликовывались как IS-95B. Именно IS-95B обычно ассоциируют с CDMA One. Наряду с голосом системы сотовой связи этого стандарта могли передавать данные со скоростями: 14,4 кбит/сек для IS-95A и 115 кбит/сек - IS-95B.

CDMA One была первой системой сотовой связи, в которой использовался кодовый метод множественного доступа (CDMA - code division multiple access). Предшествующие системы использовали частотный (FDMA - frequency division multiple access) и временной (TDMA - time division multiple access) методы множественного доступа. Все последующие после IS-95 стандарты сотовой связи, включая стандарты третьего поколения - 3G использовали CDMA при построении радио интерфейса. Таким образом, CDMA One оказалась системой-пионером в этой области.

## История CDMA One

Идея использовать распределение энергии сигнала в заданном частотном диапазоне с помощью специальной расширяющей последовательности (DSSS - direct sequence spread spectrum) для множественного доступа в мобильных системах связи пришла от калифорнийской компании Qualcomm в 1980 годах. Предыдущие DSSS – системы преимущественно использовались в военных системах связи и для спецслужб, т.к. они обладают высокой устойчивостью к обнаружению факта передачи, нарушению связи и подслушиванию разговоров.

Система предполагала перемножение (одновременную передачу в радио эфире в одном частотном диапазоне) данных с различными скоростями. Специальная последовательность, известная под названием расширяющий код (spreading code), использовалась для распределения энергии сигнала в широком частотном диапазоне = 1,25 МГц. Исходная информация может быть восстановлена лишь с использованием исходной последовательности. Таким образом, имея достаточное количество расширяющих кодов можно построить систему с множественным доступом.

С целью улучшения стандарта CDMA One был образован консорциум, в котором к компании Qualcomm присоединились два других крупнейших оператора сотовой связи Nynex и Ameritech с целью разработки первой CDMA-системы. Позднее этот союз был расширен компаниями Motorola и AT&T, которые внесли дополнительные ресурсы для ускорения разработки системы. Результатом их работы послужила публикация нового стандарта под аббревиатурой IS-95A в 1995 году под эгидой ассоциации индустрии сотовой связи (CTIA - Cellular Telecommunications Industry Association). В последствие была образована группа разработки CDMA (CDG - CDMA Development Group). Ее цель была продвигать CDMA и развивать технологии и стандарты, хотя в наши дни основные работы по стандартизации проводятся 3GPP2.

Спустя 3 года компанией Hutchison Telecom была запущена в эфир первая система сотовой связи стандарта CDMA One. Позднее сети IS-95 нашли широкое распространение в Северной Америке и странах Азии. Однако некоторые сети также были развернуты в Южной Америке, Африке, Среднем Востоке, также как и в некоторых странах Восточной Европы.

Опираясь на успех первого релиза стандарта CDMA One - IS-95A, была проведена работа по его улучшению. Основные изменения коснулись технологии передачи данных, и результатом стало увеличение максимальной скорости до 115 кбит/сек.

Система CDMA в дальнейшем была улучшена и преобразована в систему стандарта третьего поколения, которая предусматривала гораздо более высокие скорости передачи данных и новые услуги для абонентов. В результате перехода к 3G стандарт получил новое название CDMA2000, а после дальнейшего улучшения появились стандарты CDMA 2000 1x и CDMA 2000 1x ev-do (evolution data only or data optimised), которые предоставляли абонентам еще более высокие возможности, особенно в области передачи данных.

Система CDMA фирмы Qualcom рассчитана на работу в диапазоне частот 800 Мгц. Система CDMA построена по методу прямого расширения спектра частот на основе использования 64 видов последовательностей, сформированных по закону функций Уолша. Для передачи речевых сообщений выбрано речепреобразующее устройство с алгоритмом CELP со скоростью преобразования 8000 бит/с (9600 бит/с в канале). Возможны режимы работы на скоростях 4800, 2400, 1200 бит/с.

В каналах системы CDMA применяется сверточное кодирование со скоростью ? (в каналах от базовой станции) и 1/3 (в каналах от подвижной станции), декодер Витерби с мягким решением, перемежение передаваемых сообщений. Общая полоса канала связи составляет 1,25 Мгц.

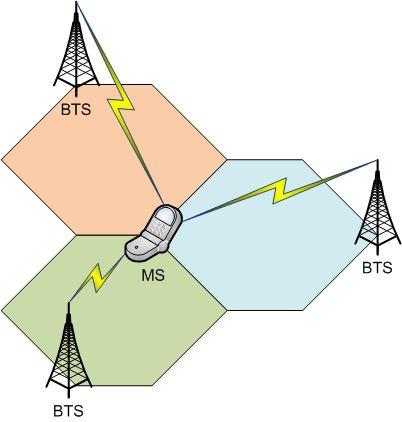
Основные характеристики приведены в таблице.

|  |  |
| --- | --- |
| Диапазон частот передачи MS | 824,040 – 848, 860 Мгц |
| Диапазон частот передачи BTS | 869,040 – 893,970 мгц |
| Относительная нестабильность несущей частоты BTS | +/- 5\*10^-8 |
| Относительная нестабильность несущей частоты MS | +/- 2,5\*10^-6 |
| Вид модуляции несущей частоты | QPSK(BTS), O-QPSK(MS) |
| Ширина спектра излучаемого  cигнала:                      по уровню минус 3 Дб                       по уровню минус 40 Дб | 1,25 Мгц  1,50 Мгц |
| Тактовая частота ПСП М-функции | 1,2288 Мгц |
| Количество каналов BTS на 1 несущей частоте | 1 пилот-канал  1 канал синхронизации  7 каналов персонально вызова  55 каналов связи |
| Количество каналов MS | 1 канал доступа  1 канал связи |
| Скорость передачи данных:  В канале синхронизации  В канале перс.вызова и доступа  В каналах связи | 1200 бит/с  9600, 4800 бит/с  9600, 4800, 2400, 1200 бит/с |
| Кодирование в каналах передачи BTS | Сверточный код R=1/2, К=9 |
| Кодирование в каналах передачи MS | Сверточный код R=1/3, K=9 |
| Требуемое для приема отношение энергии бита информации | 6-7 дБ |
| Максимальная эффективная излучаемая мощность BTS | 50 Вт |
| Максимально эффективная излучаемая мощность MS | 6,3 – 1,0 Вт |

## Особенности стандарта IS-95

Как отмечалось ранее, стандарт IS-95 использует кодовый принцип разделения абонентов (CDMA). Именно с его использованием связаны основные особенности и отличия от стандартов предыдущих поколений (NMT, AMPS, GSM и т.п.). Рассмотрим ключевые особенности стандарта CDMA One, которые дают преимущества перед системами других стандартов:

1. **Мягкая передача (Soft handoff)**. В связи с тем, что в каждой соте используются одинаковые частоты, единственное отличие между пользовательскими каналами заключается в используемой расширяющей последовательности. Поэтому, при переходе абонента из одной соты в другую нет перехода между частотами, как это было в стандартах с частотным разделением. Мобильный терминал (MS) получает аналогичный сигнал, как в соте-источнике, так и в новой соте, поэтому нет необходимость в перенастройке приемника на другую частоту. При этом мобильный терминал может получать сигнал от двух, трех и более сот. Поэтому резкое снижение качества сигнала от одной соты не приведет к разрыву соединения. В свою очередь, сразу несколько базовых станций (BTS) могут принимать сигнал от MS и контроллер базовых станций (BSC) может сравнить два и более сигнала и выбрать наилучший. Оба этих фактора снижают вероятность обрыва соединения во время хэндовера.

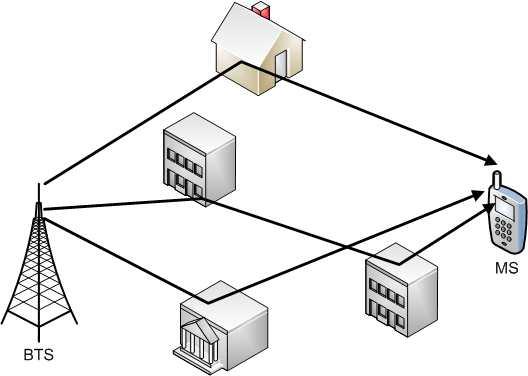


##### Пример Soft handoff с 3 базовыми станциями

2. **Гибкая емкость сети** . В системах с временным и частотным разделениями строго определено количество доступных для абонентов каналов. При этом, если система настроена соответствующе и нет проблем с работой оборудования, каналы не влияют друг на друга. Если будут попытки доступа в соту свыше числа настроенных каналов, то таким абонентам будет отказано в обслуживании.

Теоретически, это не важно: разделен ли спектр на частоты, таймслоты или коды – емкость сети будет одинаковой. Однако для CDMA все абоненты разделены с помощью кодов. Поэтому дополнительные пользователи могут быть добавлены за счет незначительного снижения качества соединений. Таким образом, емкость CDMA-систем в случае возникновения необходимость может варьироваться.

3. **Терпимость к многолучевому распространению**. Расширение спектра эффективно в борьбе с частотно-селективными замираниями, которые могут возникать при многолучевом распространении сигналов. В случае использования CDMA, энергия полезного сигнала распределяется в широкой полосе пропускания. Поэтому возникающие частотно-селективные замирания, которые являются сосредоточенными в узком частотном канале не могут нанести существенных искажений для всего сигнала. Для систем, в которых энергия полезного сигнала сосредоточена в узкой области частотно-селективные замирания могут повлечь существенное снижение качества передачи, либо даже временную блокировку каналов системы.



##### Пример многолучевого распространения сигнала

Кроме того, в CDMA One, многолучевое распространение сигнала может принести пользу для получателя сообщения при использовании, так называемого, Rake-приемника. Он принимает все переотраженные лучи сигнала и, анализируя их, может выявить ошибки и устранить их, тем самым улучшить качество связи.

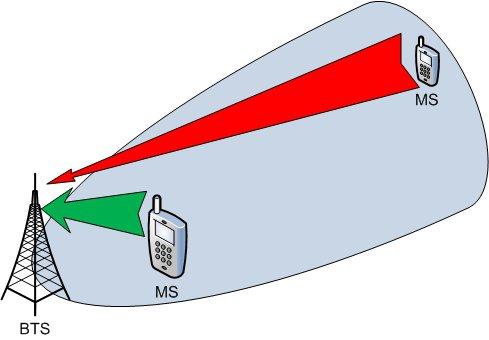
4. **Нет необходимости использовать эквалайзер**. Когда скорость передачи намного превышает 10 кбит/сек в FDMA и TDMA системах, необходимо использовать эквалайзер для снижения межсимвольной интерференции. Это связано с тем, что при увеличении скорости уменьшается длительность интервала и межсимвольные интервалы, соответственно. Поэтому энергия последующих символов может быть наложена одна на другую. В CDMA One, за счет того что энергия каждого символа передается в широкой полосе, межсимвольная интерференция не так опасна. Кроме того, значительную помощь в борьбе с этим негативным явлением оказывает Rake-приемник.

5. **Высокая скрытность и устойчивость к воздействиям извне**. Важная особенность расширенных сигналов заключается в том, что они становятся шумоподобными или псевдослучайными. Эти два термина означают, что спектр сигнала становится похож на спектр белого шума, как по форме, так и по мощности. Поэтому в эфирt такой сигнал оказывается замаскирован в покрывающих его внешних помехах и становится достаточно тяжело определить наличие сигнала, и тем более попытаться оказать на него воздействие, подслушать или подменить.

Кроме преимуществ, системы с CDMA обладают и некоторыми недостатками:

1. **Системы CDMA являются само интерферирующими**. Это означают, что работающие в эфире устройства оказывают влияние на работу других устройств, создавая им помехи. Это связано с тем, что в системе используются не совсем ортогональные (независимые) коды. Поэтому MS различных абонентов могут создавать влияние друг на друга. Причем чем больше мобильных терминалов работает в сети, тем большее влияние они оказывают друг на друга. Именно не полная ортогональность кодов является основным ограничивающим фактором для пропускной способности и емкости системы.

2. **Проблема «ближней - дальней» зон** возникает из-за того, что сигнал от MS, находящихся ближе к базовой станции претерпевает меньшее затухание, чем мобильный телефон, который находится на краю соты. Такая ситуация возникает из-за того, что энергия всех сигналов передается в общем частотном диапазоне. Это приводит к тому, что ближние мобильныt терминалы могут заглушить дальних и сократить тем самым зону покрытия соты. Основным способом борьбы с этой проблемой является управление мощностью. Обычно в системах с кодовым разделением применяется несколько различных механизмов регулирования мощностью, что позволяет снизить до минимума последствия этого явления.



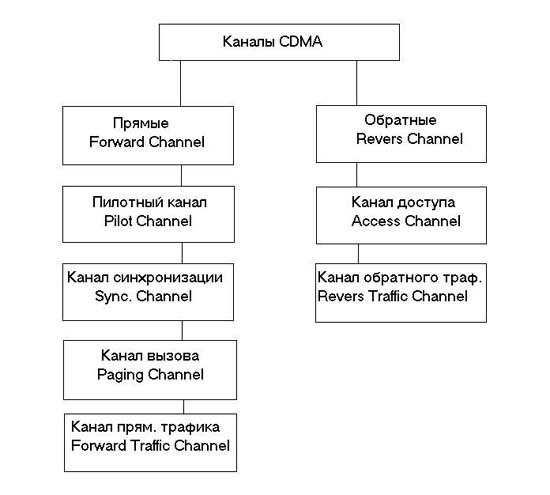
##### Проблема ближней-дальней зоны

## Стандарт IS-95 в России

История стандарта CDMA One в нашей стране достаточно богата. В первые годы повсеместного распространения сотовой связи в России (на рубеже XX-XXI столетий) было даже трудно сказать, какой из стандартов является превалирующим: IS-95 или GSM. До 2001 года в некоторые периоды CDMA имел даже большее число абонентов, чем GSM. Однако изначально в нашей стране именно стандарт GSM предусматривался как основной при строительстве сетей сотовой связи. Трудности в правовых аспектах строительства сетей CDMA One создали значительную задержку в его распространении. Хотя это не единственный сдерживающий фактор. Мобильные аппараты, работающие в стандарте IS-95 были запрограммированы на работу в определенной сети и было невозможно сменить оператора также легко, как и с MS стандарта GSM, где для этого достаточно было поменять SIM-карту.

В то же время, многие специалисты отмечают, что CDMA One гораздо экономичнее стандарта GSM и позволяет более эффективно использовать радио ресурсы. Это и другие вышеотмеченные преимущества не позволили этому стандарту быть забытым. В результате на основе CDMA One были реализованы другие стандарты уже третьего поколения.

В CDMA каналы для передачи с базовой станции называются прямыми (Forward), для приема базовой станцией - обратными (Reverse). Структура каналов в CDMA в стандарте IS-95 показана на рис:



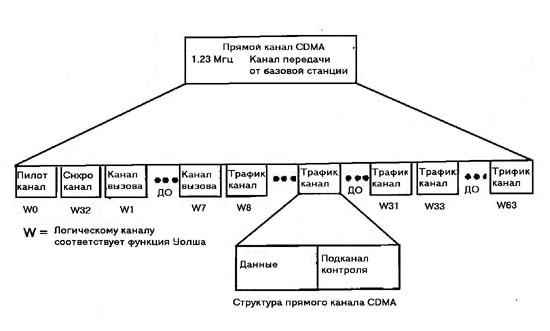
### Прямые каналы в CDMA:

1. Пилотный канал - используется подвижной станцией для начальной синхронизации с сетью и контроля за сигналами базовой станции по времени, частоте и фазе.
2. Канал синхронизации - обеспечивает идентификацию базовой станции, уровень излучения пилотного сигнала, а так же фазу псевдослучайной последовательности базовой станции. После завершения указанных этапов синхронизации начинаются процессы установления соединения.
3. Канал вызова - используется для вызова подвижной станции. После приема сигнала вызова подвижная станция передает сигнал подтверждения на базовую станцию, после чего по каналу вызова на подвижную станцию передается информация об установлении соединения и назначения канала связи. Канал персонального вызова начинает работать после того, как подвижная станция получит всю системную информацию (частота несущей, тактовая частота, задержка сигнала по каналу синхронизации).
4. Канал прямого доступа - предназначен для передачи речевых сообщений и данных, а так же управляющей информации с базовой станции на подвижную.

### Обратные каналы в CDMA:

1. Канал доступа - обеспечивает связь подвижной станции с базовой станций, когда подвижная станция еще не использует канал трафика. Канал доступа используется для установления вызовов и ответов на сообщения, передаваемые по каналу вызова, команды и запросы на регистрацию в сети. Каналы доступа совмещаются (объединяются) каналами вызова.
2. Канал обратного трафика - обеспечивает передачу речевых сообщений и управляющей информации с подвижной станции на базовую станцию.

Структура каналов передачи базовой станции показана на рис:

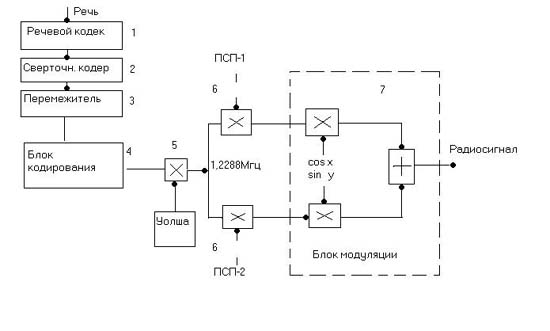


Каждому логическому каналу назначается свой код Уолша. Всего в одном физическом канале логических каналов может быть 64, т.к. последовательностей Уолша, которым в соответствие ставятся логические каналы, всего 64, каждая из которых имеет длину по 64 бита. Из всех 64 каналов на 1-й канал назначается первый код Уолша (W0) которому соответствует "Пилотный канал", на следующий канал назначается тридцать второй код Уолша (W32), следующим 7-ми каналам так же назначаются свои коды Уолша (W1,W2,W3,W4,W5,W6,W7) которым соответствуют каналы вызова, и оставшиеся 55 каналов предназначены для передачи данных по "Каналу прямого трафика".

При изменении знака бита информационного сообщения фаза используемой последовательности Уолша изменяется на 180 градусов. Так как эти последовательности взаимно ортогональны, то взаимные помехи между каналами передачи одной базовой станции отсутствуют. Помехи по каналам передачи базовой станции создают лишь соседние базовые станции, которые работают в той же полосе радиочастот и используют ту же самую ПСП, но с другим циклическим сдвигом.

### Порядок прохождения речевых данных в мобильной станции до момента отправки в эфир.

Давайте подробней рассмотрим структурную схему обратного канала трафика. В прямом и обратном канале эта схема повторяется; в зависимости от того, какой канал используется в данный момент, некоторые блоки этой схемы исключаются.



1. Речевой сигнал поступает на речевой кодек.   
   На этом этапе речевой сигнал оцифровывается и сжимается по алгоритму CELP..
2. Далее сигнал поступает на блок помехоустойчивого кодирования, который может исправлять до 3-х ошибок в пакете данных.
3. Далее сигнал поступает в блок перемежения сигнала.   
   Блок предназначен для борьбы с пачками ошибок в эфире. Пачки ошибок - искажение нескольких бит информации подряд.   
   Принцип такой. Поток данных записывается в матрицу по строкам. Как только матрица заполнена, начинаем с нее передавать информацию по столбцам. Следовательно, когда в эфире искажаются подряд несколько бит информации, при приеме пачка ошибок, пройдя через обратную матрицу, преобразуется в одиночные ошибки.
4. Далее сигнал поступает в блок кодирования (от подслушивания).  
   На информацию накладывается маска (последовательность) длиной 42 бита. Эта маска является секретной. При несанкционированном перехвате данных в эфире невозможно декодировать сигнал, не зная маски. Метод перебора всевозможных значений не эффективен т.к. при генерации этой маски, перебирая всевозможные значения, придется генерировать 8.7 триллиона масок длиной 42 бита. Хакер, пользуясь персональным компьютером, пропуская через каждую маску сигнал и преобразовывая его в файл звукового формата, потом, распознавая его на наличие речи, потратит уйму времени.
5. Блок перемежения на код Уолша.   
   Цифровой поток данных перемножается на последовательность бит, сгенерированных по функции Уолша.   
   На этом этапе кодирования сигнала происходит расширение спектра частот, т.е. каждый бит информации кодируется последовательностью, построенной по функции Уолша, длиной 64 бита. Т.о. скорость потока данных в канале увеличивается в 64 раза. Следовательно, в блоке модуляции сигнала скорость манипуляции сигнала возрастает, отсюда и расширение спектра частот.   
   Так же функция Уолша отвечает за отсев ненужной информации от других абонентов. В момент начала сеанса связи абоненту назначается частота, на которой он будет работать и один (из 64 возможных) логический канал, который определяет функция Уолша. В момент принятия сигнал по схеме проходит в обратную сторону. Принятый сигнал умножается на кодовую последовательность Уолша   
   По результату умножения вычисляется корреляционный интеграл.  
   Если Z пороговая удовлетворяет предельному значению, значит, сигнал наш. Последовательность функции Уолша ортогональны и обладают хорошими корреляционными и автокорреляционными свойствами, поэтому вероятность спутать свой сигнал с чужим равна 0.01 %.
6. Блок перемножения сигнала на две М-функции (М1 - длиной 15 бит, М2 - длиной 42 бита) или еще их называют ПСП- псевдослучайными последовательностями.   
   Блок предназначен для перемешивания сигнала для блока модуляции. Каждой назначенной частоте назначаются разные М -функции.
7. Блок модуляции сигнала.  
   В стандарте CDMA используется фазовая модуляция ФМ4, ОФМ4.

В настоящее время оборудование стандарта CDMA является самым новым и самым дорогим, но в то же время самым надежным и самым защищенным. Европейским Сообществом в рамках исследовательской программы RACE разрабатывается проект CODIT по созданию одного из вариантов Универсальной системы подвижной связи (UMTS) на принципе кодового разделения каналов с использованием широкополосных сигналов с прямым расширением спектра (DS-CDMA).

Основным отличием концепции CODIT будет эффективное и гибкое использование частотного ресурса. Как мы раньше пояснили, на широкополосный сигнал CDMA влияние узкополосной помехи практически не сказывается. За счет этого свойства в стандарте CODIT для передачи данных дополнительно будут использоваться защитные интервалы между несущими частотами.

### Пути эволюции систем третьего поколения

Требования к системам 3G наиболее полно сформулированы в рекомендациях IMT-2000 Международным союзом электросвязи (МСЭ). Наиболее важные из них:

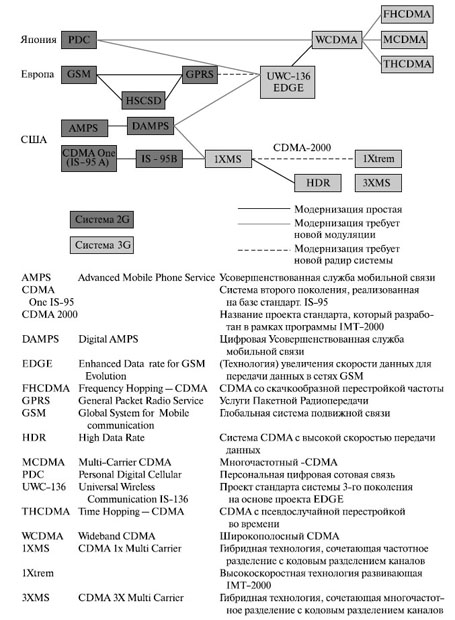
* глобальный роуминг;
* сочетание пакетной коммутации данных и коммутации каналов;
* эффективное использование спектра частот;
* открытая архитектура;
* обеспечение передачи речи, данных и мультимедийных услуг;
* качество речи, сопоставимое с проводной связью;
* защита информации, сопоставимая с уже имеющейся системой в ТфОП/ISDN;
* взаимная работа со спутниковыми системами;
* высокая скорость передачи данных;
* поддержка иерархической структуры сот (HCS — Hierarchical Cell Structure);
* поэтапный подход к повышению скорости передачи данных до 2 Мбит/с.

В Европе преобладала тенденция разработки систем на основе CDMA, совместимых с GSM (в частности, с японскими системами), но не предусматривается совместимость в глобальном масштабе.

В США имелось много сторонников эволюционного развития CDMA One к системе CDMA-2000. При этом ни один из стандартов не предполагал взаимодействия с европейской и японской системой.

Операторы DAMPS и GSM являются сторонниками дальнейшего развития систем на базе временного разделения каналов (TDMA). В результате стандарты третьего поколения (3G) взяли за основу технологию WCDMA, которую развивали европейские производители. Она, хоть и использует технологию WCDMA, не является совместимой со стандартом IS-95. Стандарты четвертого и пятого поколений также эволюционно восходят к WCDMA, таким образом американские стандарты, хоть и сделали свой вклад в дальнейшее развитие сотовых сетей, но не смогли выдержать конкуренции с европейскими производителями.

**Пути эволюции к системе 3G**



В связи с этим разрабатываемые стандарты должны предусматривать совместимость с их предшественниками. Конечная цель заключается в том, чтобы имеющиеся телефоны могли обслужить соединение при перемещении мобильной станции между сотами, базирующимися на старых и новых технологиях.Имеются различные направления эволюции.

В апреле 2007 г. Федеральным агентством связи (Россвязь) проводился конкурс на право предоставления услуг подвижной радиотелефонной связи с использованием полос частот в трех диапазонах 1935-1950 МГЦ, 2010-2015 МГЦ, 2125, 2140 МГЦ. Это по сути явилось началом внедрения услуг 3G на территории России.

# Лекция 14. Сети третьего поколения. UMTS

Широкополосный CDMA (WCDMA) — система, одобренная большинством операторов, которые способны получить новый спектр частот. Она была разработана японской фирмой ARIB в 1998 году. Одна из основных характеристик разработки — хэндовер к системе GSM. Сети GSM не могут быть модернизированы для работы с WCDMA, хотя некоторые части системы GSM, такие, как услуги пакетной радиопередачи (GPRS — General Packet Radio Service), могут многократно транслироваться через сеть CDMA.

Ширина полосы, которая отводится для одного канала WCDMA, равна 5 МГц. Возможно увеличение скорости до 10 МГц и далее до 20 МГц.

Это в четыре раза больше, чем cdma One, и в 25 раз — чем GSM. Широкая частотная полоса была выбрана, чтобы позволить более высокие скорости данных, но только в не переполненной области спектра с очень хорошим приемом. Другое важное отличие WCDMA от cdma One — отсутствие потребности в синхронизации времени. WCDMA был разработан, чтобы работать без сигналов синхронизации от глобальной навигационной системы1 (GPS — Global Positioning System). Имеются различия в кодировании: в WCDMA для кодирования используются не коды Уолша, а коды Голда. Для передачи в канал они объединяются с помощью той же QPSK-модуляции, как и в cdma One.

Все это позволяет передавать данные с максимальной скоростью приблизительно 2048 Мбит/c в пределах одной соты. Скорость в канале — 3,84 Мбит/c (7,8 и 15,6 Мбит/c). При этом предусматривается метод прямого расширения спектра (DS-CDMA).

WCDMA представляет собой систему множественного доступа с кодовым разделением каналов и прямым расширением спектра (DS -CDMA), т.е. биты информации пользователя передаются в широкой полосе частот путем умножения исходного потока данных пользователя на последовательности квазислучайных битов (называемых чипами), являющиеся кодами расширения CDMA. Для обеспечения очень высоких скоростей передачи (до 2 Мбит/с) поддерживается использование переменного коэффициента расширения и мультикодовых комбинаций.

Скорость передачи, равная 3,84 Мчип/с, приводит к занятию полосы приблизительно в 5 МГц. Системы DS-CDMA с шириной полосы около 1 МГц, например, IS-95, обычно называют узкополосными системами CDMA. Присущая системам WCDMA большая ширина полосы на несущей обеспечивает высокие скорости передачи данных пользователя, а также создает определенные преимущества в работе, например в каналах с повышенной многолучевостью. Не нарушая полученной лицензии на работу системы, оператор может иметь несколько таких несущих с полосой 5 МГц для увеличения пропускной способности, возможно, в виде ячеек иерархической структуры. Фактически такое разнесение несущих может быть реализовано и на 200 килогерцовой сетке приблизительно в полосе 4,4 и 5 МГц в зависимости от уровня интерференции несущих.

WCDMA поддерживает самые разные скорости передачи данных пользователя, другими словами, концепция получения ширины полосы по требованию (BoD) достаточно хорошо поддерживается. Каждому пользователю выделяются фреймы длительностью 10 мс, в течение каждого из которых скорость передачи данных пользователя остается постоянной. Однако пропускная способность для передачи данных у пользователя может меняться от фрейма к фрейму. На рис. 3.1 показан пример такой особенности. Быстрое выделение пропускной способности для радиосвязи будет обычно управляться сетью для достижения максимальной пропускной способности при передаче пакетированных данных.

WCDMA поддерживает два основных режима работы: частотное разделение дуплексных каналов (FDD) и временное разделение дуплексных каналов (TDD). В режиме FDD для восходящего и нисходящего каналов используются раздельные несущие с частотой 5 МГц, тогда как в режиме TDD только одна несущая 5 МГц используется для восходящего и нисходящего каналов с разделением прием-передача во времени. Восходящий канал - это канал от подвижной станции к базовой, а нисходящий - от базовой станции к подвижной. Режим TDD в значительной мере основан на концепциях режима FDD и был дополнительно введен, чтобы использовать базовую систему WCDMA так-же и для непарного (несимметричного) распределения спектра, выделенного ITU для систем IMT-2000.

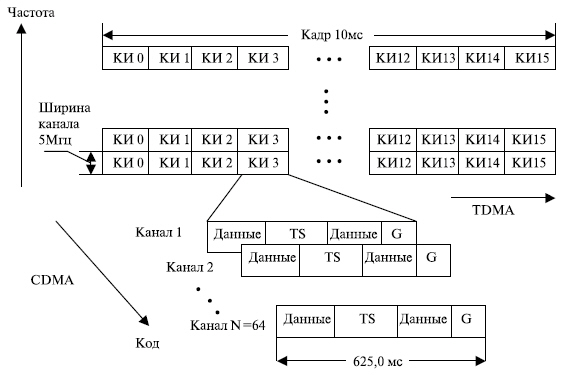
WCDMA поддерживает работу асинхронных базовых станций, так что в отличие от синхронной системы IS-95 отсутствует необходимость в глобальной привязке ко времени, например к GPS. Развертывание базовых станций внутри помещений и миниатюрных базовых станций (для пикосот) производится легче, когда не требуется получать сигнал GPS.   
WCDMA использует когерентный прием для систем WCDMA в восходящем и нисходящем каналах на основе применения пилот-символов или общих пилот-сигналов. Хотя когерентный прием уже используется в нисходящем канале в IS-95, его применение в восходящем канале является новым для систем CDMA общего пользования и приведет к увеличению общей зоны охвата и пропускной способности восходящего канала.   
Воздушный интерфейс WCDMA задуман таким образом, что оператор сети может использовать перспективные концепции построения приемников CDMA, например многопользовательский прием и применение интеллектуальных адаптивных антенн как способ повышения пропускной способности и/или зоны охвата. В большинстве систем второго поколения отсутствуют возможности использования таких концепций построения приемника, и в результате они либо не могут применяться, либо могут применяться лишь с большими ограничениями и дают лишь незначительное улучшение эксплуатационных показателей.

WCDMA предназначена для использования вместе с GSM. Поэтому поддерживаются эстафетные передачи управления (хэндоверы) между GSM и WCDMA для того, чтобы иметь возможность использовать зону охвата GSM для внедрения WCDMA.

WCDMA предоставляет возможность мягкого хэндовера, но при взаимодействии с GSM такой тип хэндовера не поддерживается.

### TD-WCDMA

TD-WCDMA (Time Division-Wideband Code-Division-Multiple-Access) звучит противоречиво и часто называется гибридом между TDMA и CDMA. При этой методике, как и в TDMA, несущая частота разбивается на канальные интервалы, но каждый канальный интервал "уплотняется" несколькими CDMA-сигналами, преобразованными с помощью ортогональных кодов (см. расширение в части 2 CDMA). В этом методе сохраняется методика мультиплексирования CDMA. Основными параметрами такой методики являются: частота, канальный интервал и код.



В UMTS для двухсторонней связи разрешено применение частотного дуплексного разделения (FDD — Frequency Duplex Division) и временного дуплексного разделения (TDD Time Duplex Division).

При FDD в различных направлениях используются различные частоты, разделенные полосой 190 МГц. Очевидно, что если спектр лимитирован, то выделение парных полос частот затруднительно.

Временное разделение (TDD) разделяет прямой и обратный поток по времени. Мобильная станция и базовая станция поочередно используют одну и ту же частоту в разных направлениях. В этом случае можно уменьшить величину занимаемой полосы и не требуется разделение спектра на парные частоты. Этот способ наиболее приемлем для небольших сот, поскольку интервал приема/передачи зависит от времени распространения информации. Однако для временного разделения часто выходом является применение асимметричных скоростей в прямом и обратном направлении. Метод TDD может оказаться более эффективным в пикосотах для работы с компьютерами (Интернет) беспроводным способом.

В WCDMA несущие частоты выделяются в соответствии с заданными методами доступа для каждой частоты. При выдаче лицензии для каждого канала указывается, должен ли он использоваться в направлении от абонента к станции или от станции к абоненту либо в непарном режиме. На рис. 5.6 показан пример разделения диапазона между операторами на 12 парных каналов и 7 непарных каналов.



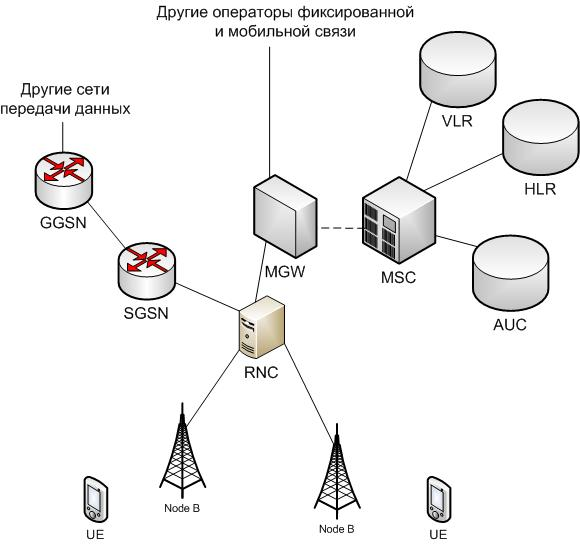
UMTS, используя разработки W-CDMA, позволяет поддерживать скорость передачи информации на теоретическом уровне до 21 Мбит/с (при использовании HSPA+). В настоящий момент самыми высокими скоростями считаются 384 Кбит/с для мобильных станций технологии R99 и 7,2 Мбит/с для станций HSDPA в режиме передачи данных от базовой станции к мобильному терминалу. Это является скачком по сравнению со значением в 9,6 Кбит/с при передаче данных по каналу GSM или использованием в соответствии с технологией HSCSD нескольких каналов 9,6 Кбит/с (при этом максимально достигаемая скорость — 14,4 Кбит/с в CDMAOne), и, наряду с другими технологиями беспроводной передачи данных (CDMA2000, PHS, WLAN) позволяет получить доступ к Всемирной Паутине и другим сервисам посредством использования мобильных станций.

Стандарты третьего поколения пришли на смену стандартам 2G. В первую очередь их появление обусловлено возросшими потребностями абонентов в скорости передачи данных. Стандарт UMTS (Universal Mobile Telecommunications System - Универсальная система мобильной связи) нашел наибольшее распространение среди других стандартов этого поколения на территории Европы, в том числе и России.

Разработка стандарта UMTS началась в 1992 году организацией по стандартизации IMT-2000. Впоследствии разработка этого стандарта была поручена 3GPP. Первая сеть UMTS была запущена в коммерческую эксплуатацию 1 декабря 2001 года в Норвегии. К маю 2010 года число абонентов переваливает за 540 миллионов по всему миру.

Рассмотрим структуру системы UMTS и ее основные отличия от стандарта второго поколения GSM.

**UTRAN** (UMTS Terrestrial radio access network) – наземная сеть радиодоступа стандарта UMTS. Представляет собой совокупность сетевых элементов, обеспечивающих доступ абонентов к услугам сотовой связи. Главной задачей UTRAN является установление соединений между UE c одной стороны и CN или пакетной сетью - с другой.



**Подсистема коммутации**

В первых релизах стандарта UMTS (R99, R4) подсистема коммутации не отличалась по своей структуре от той же подсистемы сетей второго поколения. В нее входили MSC – Mobile Switching Centre, который выполнял функции коммутации, установления соединения, тарификации и др., а также ряд регистров HLR, VLR, AUC, которые предназначены для хранения абонентских данных. В более поздних релизах (R5, R6, R7,R8) функции MSC были разделены между двумя устройствами: MSC-Server и MGW (Media gateway). MSC-Server отвечает за установление соединений, тарификацию, выполняет некоторые функции аутентификации. MGW представляет собой коммутационное поле, подчиненное MSC-Server.

**Подсистема базовых станций**

В сети UMTS по сравнению с сетью GSM наибольшие изменения претерпела подсистема базовых станций. Отмеченные выше преимущества достигаются в первую очередь за счет новой технологии передачи информации между базовой станцией и телефоном абонента.

Итак, рассмотрим основные элементы, входящие в подсистему базовых станций:

RNC (Radio Network Controller) – контроллер сети радиодоступа системы UMTS. Он является центральным элементом подсистемы базовых станций и выполняет большую часть функций: контроль радиоресурсов, шифрование, установление соединений через подсистему базовых станций, распределение ресурсов между абонентами и др. В сети UMTS контроллер выполняет гораздо больше функций нежели в системах сотовой связи второго поколения.

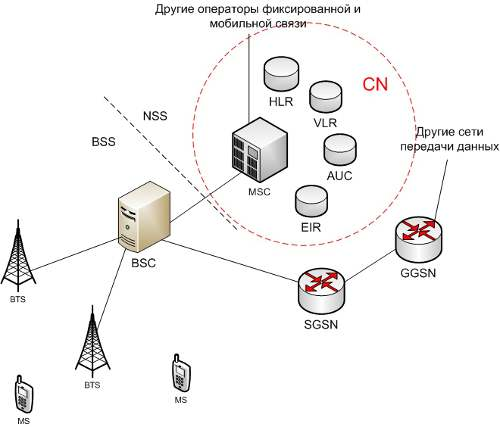
NodeB – базовая станция системы сотовой связи стандарта UMTS. Основной функцией NodeB является преобразование сигнала, полученного от RNC в широкополосный радиосигнал, передаваемый к телефону. Базовая станция не принимает решений о выделении ресурсов, об изменении скорости к абоненту, а лишь служит мостом между контроллером и оборудованием абонента, и она полностью подчинена RNC.

Оборудование абонента получило название UE (User Equipment). Тем самым подчеркивается, что в отличии от предшествующих стандартов в UMTS может быть не только обычный телефон, но и смартфон, ноутбук, стационарный компьютер и т.п.

Пакетные данные в сети UMTS передаются от MGW к известному нам по системе GSM элементу SGSN, после чего через GGSN поступают к другим внешним сетям передачи данных, например Internet. Как правило, SGSN и GGSN сети GSM применяются для тех же целей и в сети UMTS. Производится только коррекция программного обеспечения данных элементов.

### CN (Core Network)

CN (Core Network) – ядро сети сотовой связи различных стандартов. Эту сеть еще иногда коротко называют Core (ядро). Из названия уже понятно, что CN представляет собой центральную систему сети, которая предназначена для хранения абонентских данных, и отвечающая за установление соединений, аутентификацию абонентов, начисление платы за предоставленные услуги связи.



Core, на самом деле, представляет собой систему коммутации. В сетях GSM в качестве CN выступает NSS (Network switching system), в UMTS Core имеет такое же название - CN. В зависимости от стандарта и используемых в ней технологий коммутации, хранения данных и предоставляемых услуг Core содержит различные элементы. Однако основными являются: центральный коммутатор и базы данных. Центральный коммутатор предназначен для установления, поддержания и разрушения соединений, выставления счетов абонентам за оказанные услуги связи, а также проводит некоторые процедуры, необходимые для безопасного доступа и работы абонентов в сети. Базы данных служат хранилищем различной информации, необходимой для нормальной работы в сети. К таким данным, в частности, относятся местоположение абонента в сети, идентификаторы, разрешенные (запрещенные) услуги, данные необходимые для проведения различных процедур безопасности абонентов и т.п. В зависимости от стандарта набор хранимых данных и количество баз данных может меняться.

### MSC server (MSC-S)

MSC-S/С (MSC server) – коммутатор мобильной сети сотовой связи стандарта UMTS. Система коммутации (NSS) сети UMTS в отличие от сети стандарта GSM претерпела ряд изменений, одно из которых – это разделение MSC на два элемента MSC-S и MGW. На MSC остались возложены функции обработки сигнализации, установления соединений, аутентификации, начисления стоимости, межсетевого взаимодействия (Interworking). В то время как все голосовые соединения коммутируются в MGW под управлением MSC-S. В первую очередь такое разделение необходимо для повышения гибкости CN. Теперь при возросшей абонентской нагрузке достаточно расширить MGW или добавить еще один MGW, без существенных изменений в MSC-S, т.к. один MSC-S может управлять сразу несколькими MGW.

Если сеть UMTS строится на основе сети GSM, то в качестве MSC-S, как правило, выступает MSC сети 2G. Для этого на большинстве существующих коммутаторов достаточно обновить версию ПО. Причем этот же коммутатор будет выполнять, и функции MSC для GSM, и MSC-S для UMTS, и будет управлять MGW.

Основным отличием MSC UMTS от аналогичного узла MSC системы GSM является то, что коммутатор MSC должен быть рассчитан на высокие скорости, поэтому он обычно выполняется на базе ATM-коммутатора.

Основными элементами базовой сети являются:

* домашний регистр местоположения (HLR — Home Location Register), который содержит всю административную информацию каждого абонента, зарегистрированного в соответствующей сети GSM, наряду с текущим местоположением мобильных станций;
* визитный регистр местоположения (VLR — Visit Location Register). С его помощью достигается функционирование подвижной станции за пределами зоны, контролируемой HLR.

Подобно RNC, центр коммутации мобильной связи (MSC) также разработан на основе базовой АТМ-инфраструктуры и обладает такой же гибкостью, что и RNC. В действительности некоторые функции могут даже перераспределяться между RNC.

Основной задачей MSC является установление и разъединение соединений от мобильных станций. Так как MSC может в одном и том же узле обрабатывать речь, осуществлять передачу пакетных данных и данных с коммутацией каналов, становится возможным обслуживание мультимедийных приложений. MSC выполняет функции:

* адаптивной обработки как пакетных данных, так и данных для передачи с коммутацией каналов;
* взаимодействия с сетями ISDN;
* взаимодействия с локальными компьютерными АТМ-сетями;
* кодирования/декодирования речи в соответствии с рекомендациями ITU-T G.729 (при условии реализации кодеков в MSC);
* эхоподавления (echo supervision);
* IP-маршрутизации.

Для адаптивной обработки абонентских данных для передачи по аналоговым голосовым сетям, а также сетям с коммутацией каналов и с коммутацией пакетов, используется внешнее оборудование, например, конвертор ISDN и АТМ-маршрутизатор.

Внешний интерфейс основной скорости (ET BRI) соответствует стандартам. Кроме того, при подключении внешнего конвертора ISDN также могут быть реализованы европейские ISDN-интерфейсы (PRI и BRI), соответствующие рекомендациям ITU-T, Q.931 (Уровень 3), Q.921 (Уровень 2) и I.430/I.431 (Уровень 1). Внешняя локальная компьютерная АТМ-сеть использует постоянный виртуальный канал для осуществления всех подключений IP-поверх-ATM в соответствии со спецификацией IETF RFC 1483.

Возможности совместимости центра коммутации мобильной связи испытательной системы (блок IWF) позволяют подключаться к центрам коммутации сетей GSM.

Встроенный IP-маршрутизатор обеспечивает обработку потоков со скоростью до 10 Мбит/с. Распределение ресурсов между речью, канальными данными и пакетными данными регулируется различными вариантами конфигурации эхоподавителя, блоков адаптации услуг UDI (UADP) и адаптации пакетных услуг (PADP), IP-маршрутизатора (IPR) и интерфейса PRI.

Внешние сети можно разделить на две группы:

* сети c коммутацией каналов (CS — Channel Switching). Они обеспечивают соединения с коммутацией каналов, как это делается в существующей в настоящее время телефонной связи;
* сети с коммутацией пакетов (PS — Packet Switching) ( рис. 6.4). Они обеспечивают соединения с коммутацией пакетов данных. Одним из примеров сети PS служит Интернет.

### Media gateway (MGW)

MGW (Media gateway) – элемент сети сотовой связи стандарта UMTS, предназначенный для коммутации абонентской нагрузки. В сети стандарта UMTS система коммутации (CN) в отличие от сети стандарта GSM претерпела ряд изменений, одно из которых – это разделение MSC на два элемента MSC-S и MGW. MSC-S выполняет ряд функций по обработки сигнализации и управляет MGW. Весь абонентский голосовой трафик коммутируется в MGW под управлением MSC-S. Таким образом, MGW представляет собой коммутационное поле, к которому подключены интерфейсы к сети абонентского доступа и внешним голосовым сетям. Один MSC-S может управлять сразу несколькими MGW.

Главная цель разделения CN заключается в необходимости повышения масштабируемости сети. Дело в том, что как правило при возрастании абонентской нагрузки в первую очередь требует расширения часть именно касающаяся коммутации и интерфейсов к другим сетям. Так вот в сети UMTS эта задача достаточно легко решаема. Для этого достаточно добавить дополнительный MGW уже имеющемуся.

Введение MGW в структуру CN также упрощает реализацию Gateway MSC. Если появляется необходимость в шлюзовом коммутаторе, то в качестве него может выступать отдельный MGW, а управлять им может уже имеющийся у оператора MSC-S.

### Radio Network Controller (RNC)

RNC (Radio Network Controller) – контроллер сети доступа сети сотовой связи стандарта UMTS. RNC является центральным элементом сети радиодоступа (RAN –radio access network) и выполняет следующие задачи:

Управление всеми интерфейсными каналами к другим элементам сети (NodeB, MGW, MSC-S, SGSN)

Управление радио ресурсами на интерфейсе между базовой станцией (NodeB) и оборудованием абонента (UE)

Установление поддержание и разъединение соединений через RAN для голосовых, пакетных и других видов услуг.

Приоритезация пакетного трафика для различных абонентов.

Контроль качества на радио соединениях

Шифрование трафика на всех интерфейсах

Управление хэндоверами (внутри RAN, между различными RAN)

В системе базовых станций UMTS между различными RNC одной RAN предусмотрены прямые интерфейсы. Их главная цель - это организация меж-RNC хэндовера внутри одной системы без задействования ресурсов MSC-S и MGW. Это дает возможность снизить нагрузку на CN.

В отличие от BSC в сети стандарта GSM на RNC возложено гораздо больше функций. Таким образом, система базовых станций становится более централизованной, а количество функций базовых станций уменьшается, что упрощает их структуру, стоимость и тем самым упрощает масштабирование сети.

Контроллер управления радиосетью (RNC), архитектура которого показана на рис. 6.1, обеспечивает функции:

* управления радиоресурсом, обработки принятых сигналов и мягкого хэндовера;
* кодирования и декодирования сигналов (если кодеры и декодеры установлены в контроллере);
* приема и передачи информации каналов, которая поступает от мобильных станций по интерфейсу, обеспечивающему взаимодействие с ATM-системой со скоростью 1,5-2 Мбит/с (по интерфейсу Iub [106]);
* передачи информации к центру коммутации мобильной связи по ATM-каналам со скоростью 155 Мбит/с по Iu-интерфейсу;
* отсчета времени и синхронизации.

К одному контроллеру радиосети могут быть подключены как минимум три базовые станции. При этом каждая из них может использовать до двух 1,5 или 2 Мбит/с Iub-каналов. Транспортная емкость конфигурации, представленной на рис. 6.2, составляет около 160 мобильных станций, которые могут установить соединения друг к другу или к сети фиксированной связи. Каждое подключение коммутируется в MSC через ATM-коммутатор.

UMTS во время мягкого хэндовера с одним UE могут работать два контроллера RNC. Тогда один из них (завершающий соединение) называется обслуживающим (SRNS — Service RNC), а другой — дрейфующим (Drift RNC). Принцип работы и задачи станций при мягком хэндовере были изложены при описании работы сети CDMA и будут рассмотрены для UMTS далее.

### NodeB

NodeB – базовая станция сети стандарта UMTS. Она отвечает за создание покрытия сети сотовой связи. Основной функций NodeB является передача сигнала пришедшего от RNC в эфир в определенной области – соте (сотах). NodeB логически соответствует BTS сети стандарта GSM, но обладает меньшей функциональностью.

Практически каждый производитель оборудования для UMTS сетей имеет целую линейку различных вариантов NodeB для различных целей, емкостей и вариантов установки.

NodeB обычно состоят из двух основных частей: блок промежуточной частоты, который отвечает за мультиплексирование сигнала пришедшего от RNC и его перемодуляцию на промежуточную частоту. После чего этот сигнал по оптическому патчкорду (соединительному кабелю) передается к радио блоку, который уже преобразует сигнал из промежуточной частоты в высокочастотный сигнал и передает его по фидеру к секторным антеннам. Такая схема примечательна тем, что радио блоки можно устанавливать непосредственно возле антенн. Это дает значительную экономию средств, т.к. отпадает необходимость в прокладке длинной фидерной трассы, а также уменьшает потери, потому что оптический кабель вносит гораздо меньшее затухание, чем коаксиальный.

### UE (User Equipment)

UE (User Equipment) – абонентское оборудование сетей стандартов UMTS и LTE. В отличие от сетей 1G и 2G абонентские терминалы в сетях 3G и 4G не ограничиваются лишь мобильными телефонами. Модули для доступа в сеть сотовой связи можно найти в очень многих привычных нам устройствах как бытового, так и промышленного назначения. Причем это могут быть не только мобильные устройства, но и стационарные, т.к. сети UMTS и LTE предусматривают скорости передачи данных десятки или даже сотни мегабит в секунду. Это может составить конкуренцию проводным сетям передачи данных по скорости и качеству и быть гораздо более простым решением.

Также как и MS в сетях первого и второго поколений UE сети стандарта UMTS также состоит из двух составных элементов: USIM (UMTS subscriber identity module) – абонентского идентификационного модуля сети стандарта UMTS, т.е. USIM-карты и ME (Mobile Equipment) – мобильного оборудования, т.е. радио терминала, используемого для доступа в сеть. Такое разделение UE дает возможность легкой смены телефонного аппарата (другого оборудования) или оператора связи (номера телефона) без замены второго элемента UE.

UE классифицируются по многим признакам, наиболее популярным из которых является набор поддерживаемых услуг. Так UE могут быть с поддержкой видеозвонка, высокоcкоростной передачи данных HSPA (HSDPA+/- HSUPA) для сетей UMTS, потокового видео и т.п. Кроме того, UE классифицируются по максимальной скорости передачи данных.

Мобильная станция должна быть рассчитана на поддержку всех видов услуг сети третьего поколения. Она должна обеспечивать:

* передачу речи с принятым для системы набором скоростей (табл. 5.4 в "Стандарты третьего поколения" );
* услуги службы видео — видеоконференции и приложения видеотелефонии, как основанные на коммутации каналов (от установок ISDN), так и использующие передачу пакетов (TCP/IP);
* услуги сети Интернет со скоростями до 473,6 Кбит/с при работе в обычном режиме и в режиме best effort (с максимально возможной скоростью);
* удаленный доступ к корпоративным локальным сетям с передачей для работы с файловыми серверами, базами данных приложений, для совместной работы;
* приложения электронной почты.

### Каналы

Данные, передаваемые по каналам UMTS/WCDMA, организуются в виде кадров, временных положений (слотов) и каналов. Это касается всей полезной нагрузки и управляющих сигналов.

UMTS использует технологию CDMA, как и технологию доступа, но дополнительно применяет технологию временного разделения и соответственно структуру кадра и временного положения (слота) для того, чтобы обеспечить соответствующую структуру каналов.

Каналы разделяются на 10-миллисекундые кадры, каждый из которых содержит 16 слотов длительностью по 625,0 мкс. В направлении от станции к UE время разделяется так, чтобы временные слоты содержали поля с пользовательскими данными и управляющими сообщениями.

В направлении от UE при образовании каналов используется передача в одном формате данных и управляющих сообщений.

Все каналы классифицируются по трем категориям: логические, транспортные и физические. Логические и транспортные каналы определяют методы и пути передачи данных, физические переносят полезную нагрузку и обеспечивают физические характеристики сигналов. Каналы организованы так, чтобы логические каналы зависели только от передаваемой информации, а физический уровень обеспечивает, как и с какими характеристиками передается эта информация. Протокол управления доступом к среде (MAC) обеспечивает обслуживание логических каналов. Набор типов логических каналов определен для различных видов услуг передачи данных.

Логические каналы

Широковещательный канал управления (BCCH — Broadcast Control Channel) — канал от станции к UE (DL — downlink). Этот канал широковещательно передает информацию к группе UE, а также информацию о пилот-сигналах соседних сот и т. д.

Широковещательный управляющий канал оповещения (PCCH — Paging Control Channel) (от станции к абоненту). Этот канал связан с PICH (Paging Indication Channel), о котором будет сказано немного позднее, и используется для уведомления и широковещательных передач вызова.

Выделенный канал управления (DCCH — Dedicated Control Channel) (от станции к UE и обратно). Этот канал используется, чтобы доставлять специализированную информацию управления в обоих направлениях.

Общий канал управления (CCCH — Common Control Channel), (от станции UE и обратно). Этот двунаправленный канал используется, чтобы передать управляющую информацию.

Общедоступный канал управления канала (SHCCH — Shared Channel Control Channel). Этот канал двунаправленный и применяется только в режиме временного дуплексного разделения (TDD — Time Duplex Division) WCDMA/UMTS, где он используется, чтобы транспортировать общедоступную управляющую информацию канала.

Специализированный канал трафика (DTCH — Dedicated Traffic Channel). Это двунаправленный канал, используется для доставки пользовательских данных или трафика.

Общий канал трафика (CTCH — Common Traffic Channel) (от станции к абоненту) — однонаправленный канал, используется для передачи специализированной пользовательской информации группе UEs.

Транспортные каналы

Транспортные каналы передают информацию, обеспечивающую надежное и достоверное прохождение данных по сети.

Специализированный (выделенный) транспортный канал (DCH — Dedicated transport Channel) представляет собой двунаправленный канал. Он используется, чтобы передать данные конкретному UE. Каждый UE имеет собственный DCH в каждом направлении.

Широковещательный канал (BCH — Broadcast Channel) (от станции к UE). Этот канал широковещательно передает информацию к UE в соте, чтобы дать возможность им идентифицировать сеть и соту.

Канал прямого доступа (FACH — Forward Access Channel) (от станции к UE). Этот канал передает данные или информацию к UE, которая зарегистрирована в системе. В соте может быть более одного FACH. Они могут также доставлять пакеты данных.

Широковещательный канал вызова (PCH — Paging Channel) (от станции к UE). Этот канал может передавать аварийные сообщения UE, не входящие в данные вызова, SMS-сообщения, данные о сеансах связи или о типе требуемого обслуживания, например, запрос на перерегистрацию.

Канал произвольного доступа (RACH — Random Control Channel) (канал связи от UE к станции). Этот канал передает запросы на обслуживание от UE, обращающегося к системе.

Общий канал передачи пакетов (CPCH — Common Packet Channel) (канал связи от UE к станции). Этот канал обеспечивает возможности, дополняющие RACH, а также передает сигналы быстрого регулирования мощности.

Канал совместного использования (DSCH — Downlink Shared Channel) (от станции к UE). Этот канал может быть разделен между несколькими пользователями и используется для данных, которые являются "взрывными" по природе, такие как служба просмотра веб-браузеров, заявки в которую могут "взорваться" от события или по времени (например, во время чемпионата мира по футболу).

Физические каналы

Первичный общий физический канал управления (PCCPCH — Primary Common Control Physical Channel) (от станции к UE). Этот широковещательный канал непрерывно передает системную идентификацию и информацию управления доступом.

Вторичный общий физический канал управления (SCCPCH — Secondary Common Control Physical Channel) (от станции к UE). Этот канал доставляет информацию канала прямого доступа (FACH — Forward Access Channel) и широковещательного канала вызова (PCH) с сообщениями для Ues, которые зарегистрированы на сети.

Физический канал произвольного доступа (PRACH — Physical Random Access Channel) (канал связи от UE к станции). Этот канал дает возможность UE передать сообщения произвольного доступа при попытке обращения к сети.

Специализированный физический канал данных (DPDCH — Dedicated Physical Data Channel) (двусторонний). Этот канал используется, чтобы передать пользовательские данные.

Специализированный физический канал управления (DPCCH — Dedicated Physical Control Channel) (двусторонний). Этот канал доставляет управляющую информацию к и от UE. В обоих направлениях канал доставляет биты пилотного канала и идентификатор объединенного транспортного формата (TFCI — Transport Format Combination Identifier). Канал связи от станции к UE содержит также информацию управления мощностью передатчика и информацию обратной связи (FBI — FeedBack Information).

Общий пилот-канал (CPICH — Common Pilot Channel). Информация по этому каналу передается каждым узлом B, чтобы UE были способны поддерживать синхронизацию. Дополнительно эта информация должна быть использована для того, чтобы UE могли определить лучшую соту при перемещении.

Канал индикации вхождения в синхронизм (AICH — Acquisition Indicator Channel). AICH используется, чтобы сообщить UE сведения о канале данных (DCH). Может применяться для связи с узлом B — такое назначение канала возникает в результате успешного запроса службы произвольного доступа от UE.

Физический совместно используемый канал (PDSCH — Physical Downlink Shared Channel) (от станции к UE). Этот канал совместно используется для пересылки управляющей информации к UE в пределах области охвата узла B.

Канал синхронизации (SCH — Synchronizing Channel), канал синхронизации используется UE с общим каналом пилот-сигнала (CPICH —Common Pilot Channel). Информация по этому каналу передается каждым узлом B, чтобы UEs могли поддерживать синхронизацию для демодуляции сигналов. Дополнительно они могут применяться как средство определения UE лучшей соты при перемещении.

Канал индикации вызова (PICH — Paging Indication Channel). Этот канал обеспечивает информацией UE в неактивном состоянии и обеспечивает сохранность ресурсов батареи при слежении в этом режиме за широковещательным каналом вызова (Paging Channel). PICH обеспечивает UE в момент дезактивации UE.

Канал индикации состояния (CSICH — CPCH Status Indication Channel). Этот канал, который применяется только по направлению от станции к UE для передачи состояния CPCH и может также использоваться для передачи излишней нагрузки при ее всплеске или прерывистом характере.

Обнаружение конфликтов / Канал индикации назначения канала (CD/CA-ICH — Collision Detection / Channel Assignment Indication Channel). Этот канал используется в направлении от станции к UE, чтобы указать, можно ли использовать этот канал сразу или требуется активация канала.

### Общая модель протоколов UMTS

Общая модель протоколов UMTS показана на рис. 6.5. Она построена по принципу модели протоколов B-ISDN на основе взаимодействующих уровней и плоскостей.

Потоки информации, проходящие через UTRAN, логически делятся на две части:

* слой доступа (access stratum, AS) — информация, необходимая для взаимодействия UE и UTRAN;
* слой без доступа (non-access stratum, NAS) — информация, переносимая между CN и UE через UTRAN.

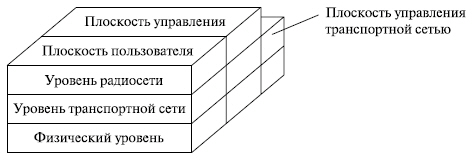
В состав слоя без доступа входят протоколы верхнего (пользовательского) уровня, которые не занимаются проблемами доступа, а связаны только с услугами.

### Плоскость управления

Протоколы плоскости управления (C-plane) определяют все функции сигнализации, установления, контроля и разъединения соединений.

Кроме этого, он включают в себя несколько прикладных протоколов, которые позволяют поддерживать сигнализацию на различных участках сети (см. рис. 6.5).

Модель протоколов UMTS



Это протоколы:

* RANAP (RAN Application) — для управления задачами сигнализации на участке радиодоступа (RNC — MSC), как часть интерфейса Iub;
* RNSAP (Radio Network System Application) — для управления задачами сигнализации на участке радиосети (на участке между RNC — RNC), как часть интерфейса Iur;
* NBAP (Network Base Station Application) — для управления задачами сигнализации на участке между базовыми станциями и RNC.

### Плоскость пользователя

Плоскость пользователя (U-plane) обеспечивает транспортировку всех видов информации в совокупности с соответствующими механизмами защиты от ошибок, контроля и управления потоком. Вся информация, передаваемая и принимаемая пользователем, например, кодированная речь при речевом вызове или пакеты при соединении с Интернетом, передаются через плоскость пользователя. Каждый поток данных характеризуется одним или несколькими протоколами фреймов, указанных для этого интерфейса.

### Плоскость управления транспортной сетью

Поскольку сеть UTRAN рассчитывается на передачу высокоскоростной информации, в наземной части она базируется на сети ATM. Для этой сети характерно, что для сигнализации используется сеть отдельных виртуальных каналов (SVC — Signaling Virtual Channel), предназначенных только для передачи сигналов управления, взаимодействия и технического обслуживания. Некоторые приложения могут требовать создания нескольких (постоянных или временных) виртуальных каналов. Например, услуги мультимедиа могут потребовать установления отдельных каналов сигнализации для услуг передачи речи, видеоизображения и данных. Каналы сигнализации могут быть односторонними или двухсторонними, симметричными (одинаковая скорость в обоих направлениях) и асимметричными (различные скорости в противоположных направлениях).

Виртуальные каналы могут быть:

* виртуальным каналом метасигнализации;
* общим широковещательным каналом;
* селективным широковещательным виртуальным каналом сигнализации;
* виртуальным каналом "точка — точка".

Плоскость управления транспортной сетью используется для управления и организации указанных выше каналов сигнализации на транспортном уровне. Она не охватывает уровня радиосети. Для сети UMTS в нее включается протокол управления звеном доступа ALCAP (Access Link Control Application), который необходим для установления транспортных B-каналов для плоскости пользователя — например, для установления каналов сигнализации "точка — точка" и для установления канала сигнализации в соответствии с услугами, предоставляемыми данному пользователю.

Когда используется плоскость управления транспортной сетью, каналы сигнализации пользователя устанавливаются по входному сообщению (транзакция) от прикладного протокола на плоскости управления, которое запускает установление этих каналов с помощью одной из частей протокола ALCAP, специально предназначенного для технологии плоскости пользователя.

Следует отметить, что протокол ALCAP может и не потребоваться, например, когда используются сети с заранее заданной конфигурацией каналов сигнализации. Тогда протокол ALCAP не запускается.

Спецификации UMTS предполагают, что запуск системы по протоколам ALCAP всегда осуществляется с помощью действий персонала по эксплуатации и обслуживанию (O&M).

### Уровень управления радиоресурсами (RRC)

RRC (Radio Resource Control) — протокол верхнего уровня [57], который является частью интерфейса Iub. Процедуры и сообщения подсистемы управления радиоресурсами приведены в табл. 6.2.

В RRC входят следующие протоколы:

* прикладные протоколы RRC;
* протоколы управления каналом связи (RLC);
* протоколы управления доступом к среде (MAC — Media Access Control).

RRC выполняет следующие функции:

* распределяет заявки по уровням на стороне пользовательского оборудования или на стороне сети UTRAN;
* выполняет широковещательные функции — широковещательное управление, доставку широковещательных сообщений;
* оповещает пользовательские терминалы (UE) о состоянии сети и радиоресурсов;
* рассылает информацию по радиосети;
* рассылает информацию всем уровням сети;
* осуществляет установление, реконфигурацию и освобождение RRC-соединения между UE и UTRAN;
* осуществляет установление, реконфигурацию и освобождение радионосителей;
* осуществляет назначение, реконфигурацию и освобождение радиоресурсов для RRC-соединения;
* обеспечивает функции мобильности соединения;
* формирует UE-сообщение о результатах измерения;
* осуществляет управление мощностью;
* управляет шифрованием;
* осуществляет выбор и перевыбор первичной соты;
* обеспечивает сохранение достоверности информации.

Уровень RRC обеспечивает соединения сигнализации к верхним уровням с целью поддержания обмена информационными потоками между процессами верхнего уровня. Сигнальное соединение используется для передачи сообщений между пользовательским оборудованием и основной сетью, чтобы передать информацию верхнего уровня. Для каждой локальной области сети сигнальное соединение может обслуживать в каждый момент только один вызов для одного UE.

# Лекция 15. HSPA

## Технология HSDPA

Рабочая группа 3GPP постоянно совершенствует стандарты IMT-2000/UMTS. Технология High Speed Downlink Packet Access (HSDPA) принадлежит к семейству решений WCDMA/UMTS, использующих пакетную передачу данных, и полностью совместима с UMTS Release 99. Это позволяет одновременно предоставлять сервисы голосовой связи и передачи данных HSDPA и UMTS. Последняя модификация технологии HSDPA позволяет получать максимальную теоретическую скорость передачи данных до 21 Мбит/с в режиме downlink transfer (от базовой к мобильной станции). Фактически HSDPA является «надстройкой» к сетям UMTS, поэтому ее нередко называют поколением 3,5G. Необходимо подчеркнуть, что протоколы HSDPA поддерживают передачу данных только от базовой станции (БС) к мобильной абонентской станции (Mobile Services, MS), получившую название «нисходящая передача данных». Обратная передача данных от абонентской станции (АС) к базовой описывается протоколами HSUPA. Подробнее об этом будет сказано далее.

В спецификации 3GPP Release 5 была впервые опубликована архитектура технологии HSDPA. В данном документе для HSDPA описаны алгоритмы адаптивной модуляции и кодирования AMC (Adaptive Modulation and Coding), а также модернизированный метод автоматического запроса повторной передачи ARQ (Automatic Request for Repeat). Отметим, что в Release 5 описаны протоколы IP версии 6 (IPv6). В этой версии добавлена также подсистема IP-мультимедиа (IMS). Домашний регистр (HLR) дополнен сервером собственных абонентов (HSS). В структуре UTRAN прописаны эффективные услуги мультимедиа на базе IP в UMTS. Кроме того, усовершенствована поддержка функции по определению местоположения (LCS).

* Совместное использование каналов, что приводит к эффективному использованию ресурсов.
* Уменьшенный TTI (transmission time interval), то есть интервал времени в течение которого можно подавать блок данных для передачи
* Адаптация связи, которая позволяет максимизировать использование канала и позволяет базовой станции управлять мощностью.
* Быстрые очереди, дающие приоритет тем пользователям, которые используют наиболее удобный канал.
* Быстрая повторная передача и мягкое комбинирования, что увеличивает ёмкость сети.
* Использование 16-QAM and 64-QAM (quadrature amplitude modulation), вследствие чего повышается пропускная способность сети.
* Использование MIMO.

### High-Speed Downlink Shared Channel

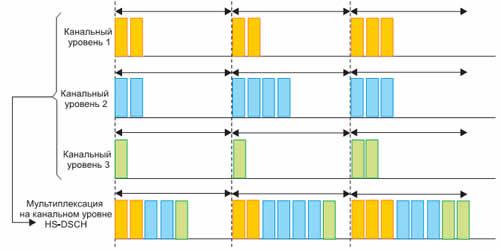
Для технологии HSDPA в спецификации стандартов 3GPP Release 5 используется новый транспортный канальный уровень High-Speed Downlink Shared Channel (HS-DSCH). В одном поддиапазоне возможна организация до 15 таких каналов с фактором распределения 16. Перераспределение каналов под задачи конкретных пользователей изменяется каждые 2 мс. Реализация этого уровня стала возможной за счет введения в стандарт трех новых физических каналов:

* HS-SCCH (High Speed-Shared Control Channel) — высокоскоростной контрольный канал для информирования пользователя об отправке данных на HS-DSCH (два верхних слота).
* HS-DPCCH (Uplink High Speed-Dedicated Physical Control Channel) — канал для подтверждения информации о доставке текущего контроля качества передачи.
* HS-PDSCH (High Speed-Physical Downlink Shared Channel) — канал, по которому физически передаются данные пользователя (в виде избыточного кода, содержащего собственно данные и дополнительные информационные биты).

### Hybrid automatic repeat-request (HARQ)

В технологи HSDPA реализован ARQ-механизм защиты от помех, при котором передача данных происходит по блокам. На приемной стороне обеспечивается контроль ошибок и генерация запроса о необходимости повторения той части информации, где они были обнаружены. В случае некорректного приема данных в новой технологии FHARQ (Fast Hybrid Automatic Repeat Request) подтверждение приема пакетов отслеживается как базовой, так и абонентской станцией. Повторные пакеты чередуются со вновь передаваемыми.

Оцифрованная информация мультиплексируется и кодируется для передачи по соответствующему физическому каналу. Схема мультиплексирования с временным и кодовым разделением в канале HS-DSCH, объединяющем три транспортных канала DCH 1-3, приведена на рис. 1. В технологии HSDPA применяются схемы модуляции QPSK (Quadrature Phase-Shifting Keying, квадратурная фазовая модуляция) и 16-, 64-QAM (Quadrature Amplitude Modulation, квадратурная амплитудная модуляция). При использовании QPSK, в зависимости от значения информационного элемента, изменяется только фаза сигнала, в то время как амплитуда и частота не меняются. При этом каждому информационному биту ставится в соответствие не абсолютное значение фазы, а ее изменение относительно предыдущего значения.



**Адаптивная перестройка манипуляции и кодирования.**

Схема цифровой манипуляции может изменяться в зависимости от качества сигнала и нагрузки на соту. Изначальной схемой выбрана QPSK, но чистая радио-среда позволяет перейти на 16QAM и 64QAM, что значительно увеличивает пропускную способность. QPSK преполагает максимальную пропускную способность в 1.8 Мбит/сек., тогда как 16QAM позволяет повысить её до 3,6 Мбит/сек. Дополнительные коды (10, 15) также могут использоваться для улучения производительности сети.

### Dual-Cell

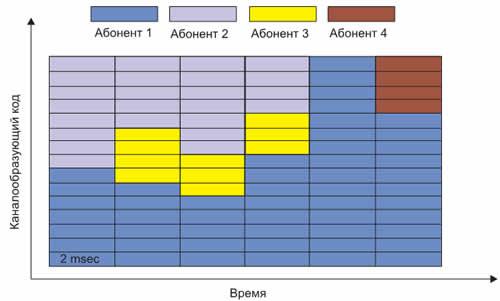
Dual Cell (DC-)HSDPA, таже известная как Dual Carrier - это эволюция HSPA подразумевающая объединения несущих при даунлинке. Dual-Carrier HSDPA – это развитие технологии HSDPA/HSPA+. Благодаря данной технологии один абонентский терминал может одновременно использовать в канале от базовой станции (downlink) две частоты по 5 МГц как единый частотный ресурс, что позволяет увеличить пропускную способность канала.

Т.е., если HSDPA это High-Speed Downlink Packet Access (высокоскоростная пакетная передача данных от базовой станции к мобильному телефону), то DC HSDPA это то же самое, но с одновременным использованием двух диапазонов частот, шириной в 5 МГц.

DC-HSDPA — это технология, которая позволяет объединять стандартные несущие частоты оператора в один непрерывный отрезок спектра и обеспечивает повышение максимальной скорости передачи данных до 42 Мбит/c (42 Мбит/c — это подсчитанная теоретически возможная скорость и пропускная способность сектора базовой станции с технологией DC-HSDPA)

В реальных же условиях в сети оператора абонент, используя модем с поддержкой функционала технологии Dual-Carrier HSDPA, будет иметь возможность увеличить скорость до двух раз по сравнению со средней скоростью загрузки в данном секторе, получаемой с использованием обычного модема HSPA+. Это достигается за счет более равномерного распределения нагрузки. В рамках одной сессии терминалу абонента может быть предоставлена пропускная способность сектора базовой станции, доступная на данный момент на обеих частотах одного сектора базовой станции.

Стандартами UMTS/HSDPA предусмотрено 20 категорий с различными значениями максимального числа одновременно используемых кодов (до 15) и типом модуляции в радиоканале QPSK или QAM. Каждой из этих комбинаций соответствует максимальная скорость передачи данных в пакетном режиме стандарта HSDPA в нисходящем направлении — от БС к мобильному терминалу. При увеличении числа позиций QAM пропускная способность канала связи увеличивается в логарифмической пропорции log264/log216/log24. Однако при этом снижается помехоустойчивость, поскольку уменьшаются разности между смежными значениями амплитуд и фаз. Пропускная способность каналов связи и скорость передачи зависят от фактора распределения (spreading factor), который определяет количество каналов связи, закодированных в один поддиапазон. Теоретически UMTS/ HSDPA позволяет назначить три таких «нисходящих» канала для одного абонента. Однако на практике не стоит забывать о том, что чем больше число пользователей, тем меньше пропускная способность.



Как правило, одной и той же сетью пользуются одновременно несколько абонентов. Скорость передачи постоянно меняется, система следит за этим и с интервалом в 2 мс автоматически регулирует мощность, подстраиваясь под условия среды. При этом приоритет предоставления каналов для получения данных от БС отдается тем пользователям, для которых поддерживается наилучшее качество сигнала. Поэтому пользователи, первыми получившие доступ к сети, пока уровень сигнала был невысок, находятся в состоянии ожидания улучшения пропускной способности.

Таблица 1 . Cкорость передачи в технологии HSDPA в зависимости от типа используемой модуляции

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Протокол | Версия 3GPP | Категория | Максимальное число кодов HS-DSCH | Модуляция | MIMO, Dua;-Cell | Коэффициент избыточности кода при максимальном битрейте | Битрейт, Мбит/с |
| HSDPA | Release 5 | 1 | 5 | 16-QAM |  | 0,76 | 1,2 |
|  |  | 2 |  |  |  |  | 1,2 |
|  |  | 3 |  |  |  |  | 1,8 |
|  |  | 4 |  |  |  |  | 1,8 |
|  |  | 5 |  |  |  |  | 3,6 |
|  |  | 6 |  |  |  |  | 3,6 |
|  |  | 7 | 10 |  |  | 0,75 | 7,2 |
|  |  | 8 |  |  |  | 0,76 | 7,2 |
|  |  | 9 | 15 |  |  | 0,7 | 10,1 |
|  |  | 10 |  |  |  | 0,97 | 14 |
|  |  | 11 | 5 | QPSK |  | 0,76 | 0,9 |
|  |  | 12 |  |  |  |  | 1,8 |
| HSPA+ | Release 7 | 13 | 15 | 64-QAM |  | 0,82 | 17,6 |
|  |  | 14 |  |  |  | 0,98 | 21,1 |
|  |  | 15 |  | 16-QAM | MIMO | 0,81 | 23,4 |
|  |  | 16 |  |  |  | 0,97 | 28 |
|  |  | 19 |  | 64-QAM |  | 0,82 | 35,3 |
|  |  | 20 |  |  |  | 0,98 | 42,2 |
| Dual-Cell HSDPA | Release 8 | 21 |  | 16-QAM | Dual-Cell | 0,81 | 23,4 |
|  |  | 22 |  |  |  | 0,97 | 28 |
|  |  | 23 |  | 64-QAM |  | 0,82 | 35,3 |
|  |  | 24 |  |  |  | 0,98 | 42,2 |
| DC-HSDPA w/MIMO | Release 9 | 25 |  | 16-QAM | Dual-Cell+; MIMO | 0,81 | 46,7 |
|  |  | 26 |  |  |  | 0,97 | 55,9 |
|  |  | 27 |  | 64-QAM |  | 0,82 | 70,6 |
|  |  | 28 |  |  |  | 0,98 | 84,4 |
| DC-HSDPA w/MIMO, HSPA++ | Release 11\* | нд | нд | 64-QAM++ | Dual-Cell++; MIMO++ | нд | 672\* |

## Технология HSUPA

Чтобы регламентировать параметры абонентских станций и определить порядок их взаимодействия с базовыми, была разработана технология HSUPA (High-Speed Uplink Packet Access) — высокоскоростная пакетная передача данных в направлении «вверх» — от абонента к БС. Работу над проектом HSUPA группа 3GPP начала еще в 2002 г. Идея стандарта была сформулирована фирмами Nokia, Samsung, Sony Ericsson и другими лидерами мирового рынка мобильных телефонов и звучала как «максимальная скорость при максимальном радиусе действия и минимальном энергопотреблении». Эта идея была технически сформулирована в 3GPP Release 6. К сожалению, принципиальные различия между передачей данных «вверх» (от АС к БС) и «вниз» (от БС к АС) не позволяют просто использовать всю архитектуру и профили технологии HSDPA для MS (мобильные бытовые телефоны, базовые модули и законченные терминалы). Основная проблема согласования процессов передачи «вверх» и «вниз» заключается в потребляемой мощности. На базовой станции отбираемая мощность передатчика не ограничена в пределах действующих нормативов. Поэтому разработчики оборудования для БС могут совершенствовать технологии передачи, не задумываясь о проблемах потребляемой мощности. Для бытовых мобильных телефонов, которые составляют основную часть этого рынка, потребляемая мощность является одним из основных критериев выигрыша в конкурентной борьбе. При разработке HSUPA были использованы методы как временного, так и канального кодирования. Поскольку значительная часть энергопотребления базовой станции HSDPA приходится именно на эти блоки модуляции, данный метод в чистом виде не может быть использован для HSUPA. Поэтому в технологии HSDPA была введена функция коррекции мощности передачи в зависимости от условий среды. Это позволяет сохранить скорости передачи при перегрузках в сети в условиях интенсивных помех. Но это оборудование тоже достаточно энергоемкое. Проблема энергопотребления возникает и при модуляциях. При использовании QAM для улучшения пропускной способности нужно увеличивать ее уровень, но при этом возрастают сложность оборудования и энергопотребление. Другая проблема связана с поэтапной передачей движущейся АС (soft handover). В этом случае принимающая БС должна отслеживать меняющийся сигнал клиента и передавать его другой станции, обеспечивающей лучшие условия приема. Согласно основному варианту спецификации Release 6, в технологии HSUPA использованы модифицированные принципы, использованные при разработке технологии HSDPA. Однако технология передачи данных «вверх» отличается от технологии передачи «вниз». В редакцию HSUPA 3GPP Release 6 по сравнению с Release 5 были внесены следующие изменения:

* Добавлены новые объекты МАС-уровня (управления доступом к среде передачи данных):
* MAC-e/es в блоке АС;
* MAC-es в блоке БС;
* MAC-es на контроллере радиосети.
* В транспортном канале введен новый расширенный выделенный канал передачи данных E-DCH.
* Добавлен выделенный физический канал E-DPCH (Dedicated Physical Channel). В нем мультиплексированы два физических канала: DPDCH (Dedicated Physical Data Channel) и DPCCH (Dedicated Physical Control Channel). Кроме того, добавлены расширенный канал индикации сообщения о доставке (E-HICH), управляющий канал регулировки мощности относительно опорного уровня (E-RGCH) и канал для автоматического регулирования абсолютного значения мощности абонентской станции (E-AGCH).
* Время инкапсуляции и формирования пакетов данных сокращено до 2 мс. Однако оставлена возможность использования и TTI, равного 10 мс.
* Значение коэффициента расширения (SF) принято равным 2.
* Увеличена скорость повторной передачи на первом уровне.
* Для контроля факта доставки данных использован гибридный метод HARQ.
* Введено жесткое управление доступом к эфиру и скоростью передачи со стороны БС.
* Реализованы новые протоколы фрейма, ускоряющие работу Iub и IuR. Интерфейс Iub соединяет БС с блоком контроллеров, а IuR поддерживает сигнальный протокол RNSAP (Radio Network Subsystem Application Part). По этому интерфейсу организуют связь между обслуживающим (Serving) SRNC и пассивным (Drift) контроллером DRNC. При выполнении хэндовера SRNC осуществляет управление радиоканалами (radio link mapping).

В технологии HSUPA для передачи данных от абонента к базовой станции применяются расширенные выделенные каналы (Uplink Enhanced Dedicated Channel, UE DCH), которые позволяют использовать тот же метод линейной адаптации (Link Adaptation Method, LAM), что и в технологии HSDPA. В свою очередь, этот метод дает возможность реализовать в технологии HSUPA модель ортогонального частотного разделения каналов. При этом последовательный поток информации разбивается на отдельные блоки и символы. Символы разных блоков передаются параллельно, каждый на своей поднесущей частоте. Преимущество данного метода в том, что он позволяет снизить до минимума межсимвольные искажения, возникающие в радиоканале. За счет уменьшения размеров блока данных удалось сократить время инкапсуляции и формирование пакетов данных.

На первом уровне в структуре HSUPA введены новые физические каналы:

* E-AGCH (Absolute Grant Channel) — канал с абсолютным значением ограничения мощности абонентской станции, определяющий опорный уровень;
* E-RGCH (Relative Grant Channel) — канал регулировки мощности относительно заданного значения;
* F-DPCH (Fractional-DPCH) — частичный выделенный физический канал, являющийся модернизированным вариантом канала DPCCH, адаптированным для высокоскоростной пакетной передачи данных вверх;
* E-HICH (E-DCH Hybrid ARQ Indicator Channel) — индикаторный канал;
* E-DPCCH (E-DCH Dedicated Physical Control Channel) — контрольный канал передачи данных;
* E-DPDCH (E-DCH Dedicated Physical Data Channel) — контрольный канал состояния данных.

В стандарте HSUPA модернизированы протоколы, обеспечивающие управление ресурсами канала и отвечающие за установление, поддержание и разрыв низкоуровневых соединений, динамический выбор частотных каналов и др. В блоке АС на уровне МАС добавлен подуровень, который отвечает за контроль доставки и покадровый формат данных в процессе их передачи. В блоке БС также введены изменения в уровне, контролирующем факт получения данных. В блок контроллеров (S-RNC) добавлен уровень (MAC-es), поддерживающий повторный запрос на получение данных в случае ошибки. Кроме того, этот уровень обеспечивает совместную обработку данных, полученных от базовых станций в процессе эстафетной передачи (handover) для одного и того же абонента. Для ускорения работы интерфейсов Iub/IuR также добавлен новый протокол. Кроме того, в HSUPA изменены протоколы управления доступом к среде передачи для БС (MAC-e), АС (MAC-e/es) и блока управляющих контроллеров (MAC-es):

* MAC-e структурирован в блоке базовой станции, он вводится отдельно для каждой абонентской станции и регулирует ее взаимоотношения с базой. В рамках этого протокола АС запрашивает разрешение на связь с БС и управляет работой повторной передачи в случае ошибки.
* MAC-es в обслуживающем контроллере также вводится персонально для каждой абонентской станции. Он объединяет и преобразовывает протокольный блок данных (Protocol Data Unit) уровня MAC-es в соответствии с кодировками и номерами каждого кадра и подкадра, а также поддерживает операцию дизассемблирования протокольного блока данных MAC-es.
* MAC-e/es для абонентской станции отвечает за сопровождение метода гибридного контроля подтверждения получения данных; мультиплексирование данных и присвоение идентификационной кодовой последовательности абонента (Transmission Sequence Number, TSN); осуществляет выбор транспортного формата передачи данных на основе полученного статуса выхода в эфир.

При передаче данных от абонента к станции, когда используется расширенный выделенный канал, два кодированных композитных транспортных канала CCTrCH используются одновременно. Транспортный канал может быть сконфигурирован так, чтобы время инкапсуляции (интервал передачи) составляло 10 или 2 мс. При этом заданный интервал передачи 10 мс обязательно должен поддерживаться всеми абонентскими станциями, допущенными к работе в сети, а интервал передачи 2 мс является опционным. Каждая АС может иметь только один транспортный выделенный канал передачи данных в конкретный момент времени.

Транспортный блок E-DCH (расширенный выделенный канал) на физическом уровне нагружен на канал E-DPDCH, который работает со временем инкапсуляции 10 или 2 мс. В основополагающей спецификации Release 6 для канала E-DPDCH используется модуляция QPSK. В спецификации Release 7 есть возможность использовать 4-PAM (Pulse Amplitude Modulation, импульсная амплитудная модуляция). Различные модификации модуляций отражены в последующих спецификациях Release 8-11.

Поскольку при передаче данных по DPCCH сначала передаются вспомогательные символы и последовательность символов (RSN), то на уровне E-DPDCH не может быть передана никакая другая информация, кроме полезных символьных данных. Для увеличения скорости передачи в канале E-DPDCH применяются комбинации мультикодов. При этом используются ортогональные коды с переменным коэффициентом расширения, равным 2. В принципе, возможны и другие варианты кодов с переменной длиной, определяемой коэффициентом расширения спектра SF. Такие коды формируются на основе заданного алгоритма, и каждый последующий уровень удваивает число возможных кодовых комбинаций. Различные наборы кодов обуславливают различные скорости передачи. Так, например, один код с коэффициентом расширения SF4 соответствует скорости передачи 960 кбит/с. Два кода с коэффициентом расширения SF4 дают скорость 1920 кбит/с. При использовании кода с коэффициентом расширения SF4 в трех параллельных каналах скорость увеличивается до 5760 Кбит/с.

Выделенный контрольный канал (E-DPCCH) предназначен для переноса информации о подтверждении получения переданных абонентской станцией данных. По этому каналу передаются:

* информация о расширенном транспортном формате передачи данных, которая составляет 7-битную последовательность и определяет скорость передачи данных;
* дополнительные два бита, содержащие данные о повторной передаче (при этом RSN сообщает, является пакет новым или повторной передачей ранее отправленного).
* последний бит, который дает разрешение или запрещение абонентской станции использовать более высокую скорость передачи по направлению «вверх» (от абонента к БС).

Для случая, когда время инкапсуляции равно 2 мс, десять информационных битов закодированы в 30 битах трех последовательных временных интервалов. В варианте со временем инкапсуляции в 10 мс контент подкадров с TTI, равным 2 мс, просто продублирован пять раз. Выделенный канал индикации сообщения о доставке (Hybrid ARQ Indicator Channel, HICH) может использоваться несколькими абонентами одновременно. Чтобы различать сигналы каждого пользователя, в сетях с кодовым разделением используются специальные кодовые последовательности символов, называемые индивидуальными ортогональными подписями. В сетях HSUPA каждому пользователю выделяется одна ортогональная подпись для канала E-HICH и одна — для E-RGCH. Поскольку на HICH доступно всего 40 ортогональных подписей, то только 20 пользователей могут совместно использовать один кодовый канал в каждый определенный момент времени. Управляющий канал относительной регулировки мощности для абонентской станции E-RGCH предназначен для того, чтобы повысить или понизить выходную мощность передатчика АС. По данному каналу не передается точное значение мощности, которую абонентская станция должна установить. Базовая станция отслеживает сигнал АС и регулярно сообщает ей текущий статус, относительно которого АС должна регулировать свою работу. В случае если связь ухудшается, БС выдает команду на увеличение мощности передачи АС. В том случае, когда абонентов в сети мало и сигнал АС достаточно сильный, БС посылает управляющий сигнал на уменьшение мощности.

Канал абсолютной регулировки мощности E-AGCH предназначен для того, чтобы установить верхний предел мощности передатчика абонентской станции, который может быть задействован в данный конкретный момент. Максимальная мощность напрямую связана с максимальной скоростью передачи данных. В отличие от метода относительного регулирования мощности, абсолютное ограничение задается достаточно редко, когда АС запрашивает канальные ресурсы и когда устанавливается несущая частота.

По каналу E-AGCH базовая станция передает два вида сообщений:

* точное значение уровня ограничения мощности (Absolute Grant value);
* характер ограничения мощности (Scope AG). Scope AG указывает на то, будет ли значение Absolute Grant использоваться только в методе гибридного контроля подтверждения получения данных (HARQ) или в других процессах также.

При запросе на установление соединения с базовой станцией абонентская станция передает информацию о своих технических возможностях. В зависимости от них БС устанавливает для конкретной АС соответствующий режим связи.

Как уже было сказано выше, в технологии HSUPA использован HARQ (гибридный метод автоматического запроса повторной передачи). Базовым в этом варианте является метод Stop and Wait, который означает, что перед началом трансляции нового блока данных передатчик ожидает подтверждения об успешном приеме предыдущего.

Как правило, этот способ используется в режиме OFDMA, который позволяет выделить специальный канал для подтверждения передачи. Если HARQ включен, каждый пакет, переданный БС, требует от АС подтверждения получения по специальному обратному каналу. В тех случаях, когда пришло сообщение об ошибке или подтверждение успешного приема не получено в установленный срок, базовая станция приступает к повторной передаче. С этой целью можно использовать два метода. В одном случае применяется так называемый метод передачи с увеличивающейся избыточностью (Incremental Redundancy, IR). При подключении функции HARQ для каждого исходного пакета в канальном кодере формируется до четырех субпакетов, каждый со своим идентификатором (SPID). Если произошел сбой, повторно транслируется субпакет с другим SPID, который имеет тот же самый кодированный исходный пакет, но с иными параметрами кодера. В методе с «управляемым комбинированием» (Chase Combining, СС) в случае возникновения ошибки осуществляется повторная трансляция одного и того же кодированного пакета. Этот метод может использоваться только с мобильными абонентскими станциями. В варианте HSUPA при передаче от АС к БС, как отмечалось выше, используется принцип приоритетов. Первоначально абонентская станция запрашивает разрешение на начало передачи. Базовая станция принимает решение, сколько и какие именно станции будут участвовать в сеансе связи. Также в режиме передачи «вверх» реализован вариант работы по расписанию (scheduled mode), при котором АС выходит на связь в заранее оговоренное время. Предусмотрен режим работы в экстренных ситуациях.

Следует также отметить улучшенную систему контроля качества передачи данных (QoS). Блок контроля качества может обслуживать до 15 логических каналов, которые мультиплексируются на одном PDU-уровне. При этом у каждого логического канала могут быть свои различные значения QoS и различные приоритетные уровни. В настоящее время стандарты 3GPP (Release 6-11) регламентируют девять категорий технологии HSUPA, которые имеют различный набор параметров и определяют технические характеристики и свойства конкретной АС (мобильного телефона или терминала). Категории мобильных абонентских станций, поддерживающих технологию HSUPA, показаны в таблице 2 [14]. Видно, что скорость передачи данных определяется комбинацией базовых параметров оборудования, таких как CT, SF, TTI, MTW TTI.

Таблица 2. Скорость передачи в технологии HSUPA для различных категорий абонентских станций

|  |  |  |
| --- | --- | --- |
| Наименование категории абонентской станции в соответствии со стандартами 3GPP | Максимальная скорость передачи от абонента к базовой станции, Мбит/с | Наименование коммерческой версии абонентской станции, доступной в свободной продаже |
| Category 1 (3GPP Rel 99) | 0,73 |  |
| Category 2 (3GPP Rel 2) | 1,46 |  |
| Category 3 (3GPP Rel 3) | 1,46 |  |
| Category 4 (3GPP Rel 4) | 2,00 | Nokia: X3-01, N8, C5, C3-01, E52, E72, E55, 6700 Classic, N900, 5630 XpressMusic; BlackBerry: Storm 9500, 9530; HTC: Dream, Passion (Nexus One)[3]; Sony Ericsson: C510, C903, W705, W995, T715; Samsung: Wave, Wave II |
| Category 5 (3GPP Rel 5) | 2,93 | Qualcomm 6290 |
| Category 6 (3GPP Rel 6) | 5,76 | BlackBerry Tour 9630, Nokia CS-15, Option GlobeTrotter Express 441/442, Option iCON 505/505M, Samsung i8910, Apple iPhone 4, Huawei, E180/E182E/E1820/ E5832/EM770W, Micromax A60 |
| Category 7 (3GPP Rel 7 ) | 11,5 |  |
| Category 8 (3GPP Rel 8) | 11,5 | Параметры модуляции: 2 ms, dual cell E-DCH operation, QPSK only, 3GPP Rel 9 TS 25.306 |
| Category 9 (3GPP Rel 9) | 23 | Параметры модуляции: 2 ms, dual cell E-DCH operation, QPSK and 16QAM, 3GPP Rel 9 TS 25.306 |
| Category 11/12 (3GPP Rel 11)\* | 70\* |  |

Приведенные в таблице данные показывают, что чем выше категория абонентской станции, тем выше ее скорость передачи. Максимальная теоретическая скорость, с которой АС может передавать данные на БС, на сегодня составляет 23 Мбит/с. Однако это теория. Еще раз подчеркнем, что скорость передачи является переменной величиной, которая в каждый конкретный момент времени зависит от возможностей абонентской станции (мобильного телефона, смартфона, базового модуля), оборудования базовой станции и от загрузки сети.

## Высокоскоростные сети HSPA

Метод высокоскоростной пакетной передачи данных (High-Speed Packet Access, HSPA) объединяет две рассмотренные выше технологии: HSDPA (передача данных от базовой станции к абоненту) и HSUPA (передача данных от абонента к базовой станции). В стандарте 3GPP Release 8 была разработана усовершенствованная технология, получившая название Dual-Cell HSDPA. Теоретически, этот метод позволяет удвоить скорость передачи данных от БС к абоненту за счет использования удвоенной пропускной способности. Идея этой технологии заключается в том, что в сети HSDPA эксплуатируются две различные радиочастоты. Если задействовать их вместе, то появляется возможность получить два одновременных канала передачи данных «вниз». Это напоминает методику, которая применяется в некоторых маршрутизаторах Wi-Fi. Как было отмечено ранее, в сетях третьего поколения выделяются непрерывные полосы частот в определенном частотном диапазоне. Например, в России две непрерывные полосы по 15 МГц в диапазонах 1935-1980 и 2125-2170 МГц выделены для организации трех каналов в режиме частотного дуплекса (IMT-DS). Непрерывный участок шириной 5 МГц в полосе радиочастот 2010-2025 МГц отведен для организации одного канала в режиме временного дуплекса (IMT-TC). Существуют сценарии, когда одна из полос остается свободной в течение некоторого промежутка времени. Технология Dual-Cell HSDPA позволяет ее задействовать в качестве дополнительного канала передачи данных.

В стандарте 3GPP Release 9 регламентирована технология HSPA+ (Evolved High-Speed Packet Access), представляющая собой улучшенный вариант HSPA, в котором уже присутствуют более сложные модуляции 16-QAM (Uplink)/ 64-QAM (Downlink) и технология MIMO (Multiple Input Multiple Output, мультивход/мультивыход). В MIMO используются несколько приемных и передающих антенн, которые разнесены между собой таким образом, чтобы достичь наименьшей корреляции между соседними антеннами. В общем случае в методе MIMO поток данных пересылается одновременно, с использованием разных антенн. При этом антенны передают данные независимо друг от друга на одной и той же частоте. Таким образом реализуется несколько пространственно разнесенных подканалов, по которым данные передаются одновременно в одном и том же частотном диапазоне. Усовершенствованная сеть HSPA+ может теоретически поддерживать скорости до 28 Мбит/с «вверх» и до 42 Мбит/с «вниз». В принципе, возможно использование технологии DC-HSDPA в комбинации с MIMO. Кроме того, нет категорического запрета на использование различных частот при объединении полос в DC-HSDPA. Расширенные варианты технологии HSPA+ в совокупности с методом MIMO позволяют в разы увеличить скорости передачи как «вверх», так и «вниз».

# Лекция 16. LTE

**3GPP Long Term Evolution** (LTE) (долговременное развитие) — проект разработки консорциумом 3GPP стандарта усовершенствования технологий мобильной передачи данных CDMA, UMTS. Эти усовершенствования могут, например, повысить скорость, эффективность передачи данных, снизить издержки, расширить и улучшить уже оказываемые услуги, а также интегрироваться с уже существующими протоколами. Скорость передачи данных по стандарту 3GPP LTE в теории достигает 326,4 Мбит/с (демонстрационно 1 Гбит/с на оборудовании для коммерческого использования) на приём (*download*) и 172,8 Мбит/с на отдачу (*upload*); в стандарте же установлены 173 Мбит/с на приём и 58 Мбит/с на отдачу.

Стандарт 3GPP LTE, под которым чаще всего имеется в виду его версия 9 и более ранние, формально не является стандартом беспроводной связи четвёртого поколения (4G), так как он не удовлетворял всем условиям Международного союза электросвязи относительно 4G. Однако стандарт LTE Advanced, под которым понимается релиз 10 и более поздние релизы LTE, утвержден МСЭ как стандарт, отвечающий всем требованиям беспроводной связи четвёртого поколения, и включен в IMT-Advanced. Стандарт *3GPP LTE* стали относить к *pre-4G*, то есть предварительной версии стандартов 4-го поколения.

Вместе со стандартом WiMAX Release 2 (или просто WiMAX 2, что чаще используется как название стандарта IEEE 802.16m) LTE Advanced являются на данный момент всеми стандартами, утвержденными в IMT-Advanced.

В отличие от других стандартов мобильной связи LTE не привязан к какому-то конкретному диапазону частот. В этом его сила. Разработчики (3GPP) определили более 30 диапазонов, для которых производители могут выпускать стандартное радиооборудование LTE. Сюда попали как частоты, используемые сейчас под другие стандарты (например, 900, 1800 (GSM), 2100 (UMTS), 2500 (WiMAX), так и “новые”, например 700-800 Мгц (так называемый “цифровой дивиденд”). Понятно, что далеко не все из возможных диапазонов найдут широкое распространение в мире. Скорее всего, в итоге “выживет” не больше 4-5 диапазонов. Большее количество очень трудно реализовать в одном абонентском девайсе, а это уже проблема для обеспечения глобального роуминга. Если спросите, на какие диапазоны сделать ставку, мои предпочтения следующие:

* 800 Мгц (3GPP band 20) – выделен или планируется под LTE практически во всех европейских странах, включая Россию; выгоден с точки зрения затрат на обеспечение сплошного покрытия; оборудование выпускается всеми ведущими производителями;
* 2,5 Ггц (3GPP band 7) – выделен или планируется под LTE практически во всех странах Европы и Азии, включая Россию; выгоден при обеспечении емкости в хот-спотах; оборудование выпускается всеми ведущими производителями.
* 1800 Мгц (3GPP band 3) – будет освобождаться по мере уменьшения количества GSM-only телефонов и расширения покрытия 3G (чтобы было, куда переводить голос); хорош с точки зрения обеспечения в сети баланса между емкостью и покрытием; GSM-операторам даст возможность сэкономить за счет переиспользования инфраструктуры сети доступа (приемопередатчики, антенны); оборудование выпускается почти всеми ведущими производителями

Вообще, выбор правильного диапазона для развития LTE – задача не из простых. В нижних диапазонах, где всё отлично с покрытием, проблема найти полосу достаточной для полноценного LTE ширины. В верхних обычно хорошо с частотным ресурсом, но БС нужно ставить через каждые 400-500 метров, разоришься на сплошном покрытии! Вероятно, большинство сетей LTE, аналогично GSMу, будут двух-диапазонные.

#### Про скорости

Максимальные скорости передачи данных – ключевой показатель крутости стандарта для конечных пользователей. Можно долго говорить о теоретических возможностях разных стандартов, перспективах их развития и так далее, но то, что абонентам в уже работающих сетях LTE доступны скорости более 100 Мбит/с – это факт. И это только начало светлого будущего: уверен, что достижение в сетях LTE скоростей до 1 Гбит/с – вопрос нескольких лет. Дальше посмотрим. Скорее всего, нужен будет очередной прорыв, как в теории радиосвязи, так и в технологии производства элементной базы.

#### Про покрытие

Зона покрытия одной БС в LTE может быть абсолютно разной. От чего это зависит прежде всего? От используемого диапазона частот. Если сравнить крайние варианты, то площадь покрытия одной eNodeB, работающей в самом нижнем LTE-диапазоне (700 Мгц) оказывается, при прочих равных, в 5-6 раз больше, чем для базы, работающей в 2.5 ГГц. В условиях городской застройки радиус соты, таким образом, может быть от нескольких сот метров до нескольких километров. Что касается рекорда по дальности действия БС LTE, он был установлен в ходе трайла греческого оператора Cosmote на оборудовании Huawei в начале этого года – на расстоянии 102 км от БС была получена скорость передачи 135 Мбит/с. Конечно, это была прямая видимость и один абонент в соте. Но с точки зрения предельных возможностей стандарта – довольно убедительно.

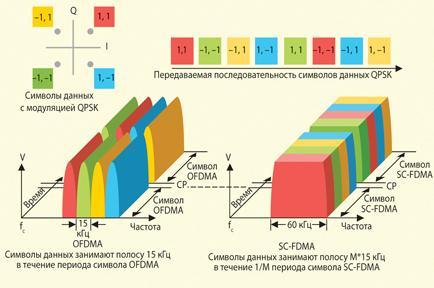
Для обеспечения двунаправленной передачи данных между БС и МС технологией LTE поддерживается как частотный (FDD), так и временной дуплекс (TDD). Для частотного дуплекса определено 15 парных частотных диапазонов (частоты от 800 МГц до 3.5 ГГц), а для временного - 8. При этом, ширина радиоканала может быть различной. Допустимы следующие значения: 1.4, 3, 5, 10, 15 и 20 МГц. В качестве систем множественного доступа в LTE используются OFDMA (Orthogonal Frequency-Division Multiple Access) в нисходящем канале и SC-FDMA в восходящем канале.

При использовании технологии **OFDMA** весь имеющийся спект разбивается на поднесущие, ортогональные друг другу. В зависимости от используемой ширины канала общее количество поднесущих может быть 72, 180, 300, 600, 900 или 1200. Каждая из поднесущих может иметь свой вид модуляции. Могут использоваться следующие модуляции: QPSK, 16QAM, 64QAM. Множественный доступ организуется за счет того, что одна часть поднесущих выделяется одному пользователю к кадре, другая часть - второму пользователю и т.д. Для более подробной информации см. описание физического уровня.

Основной плюс технологии OFDMA заключается в том, что она позволяет бороться при приеме сигнала с негативными эффектами, вызванными многолучевым распространением. Однако, этой технологии так же присущи и некоторые недостатки. Основные из них заключаеются в том, данная технология очень чувствительна к синхронизации по частоте. А также, сгенеренный OFDMA сигнал обладает высоким PAPR (Peak to Average Ratio). Это в свою очередь сказывается на том, что используемый усилитель сигнала будет работать в нелинейных участках своей характеристики. Поэтому его эффективность будет низкой, что достаточно критично для устройств с ограниченным запасом энергии (мобильных терминалов). Из-за этого в восходящем канале LTE используется другая технология множественного доступа, а именно SC-FDMA (Single Carrier Frequency Division Multiple Access). Отличие SC-FDMA от OFDMA заключается в том, что в SC-FDMA используется дополнительная обработка сигнала для снижения PAPR. В SC-FDMA в качестве такой дополнительной обработки сигнала используется преобразование Фурье. Так же, как и в нисходящем канале, в восходящем канале могут использоваться следующие виды модуляции: QPSK, 16QAM, 64QAM.

## OFDM

В радиочасти применены новые методы модуляции: OFDM на downlink и SC-FDMA на uplink. Технология MIMO которая применялась и в HSPA+(2х2 антенн), получила дальнейшее развитие (4х4 антенн и более, в зависимости от релиза 3GPP и поддержки терминалами).



Всё это помогло получить большую пропускную способность радиоинтерфейса *(300 Mbit/s на Downlink и до 75 Mbit/s на Uplink)*. Забегая вперед, скажу, что на тестовой базе мы получали скорости **80 – 85 Mbit/s** на downlink.

Нельзя не упомянуть методы доступа с частотным (FDD) и временным (TDD) разделением каналов, которые вместе с разными несущими частотами мешают нам пользоваться одним терминалом, например в России и США. Хотя ведущие производители LTE-оборудования уже интегрируют обе технологии в одном чипе, что позволит избежать указанных неудобств.

Преимущество FDD – более низкая интерференция между соседними BS и более высокая скорость в Downlink на одинаковой с TDD ширине канала *(скорость downlink в TDD на канале 20 МГц соответствует скорости в FDD на канале 15 МГц)*. TDD с другой стороны, более эффективно использует ресурсы при асимметричном канале *(каким и является канал в мобильной связи)*, поскольку в TDD возможно регулировать соотношение ресурсов для downlink/uplink. Поэтому, как FDD, так и TDD нашли своё место в современных сетях LTE.

**MU-MIMO**

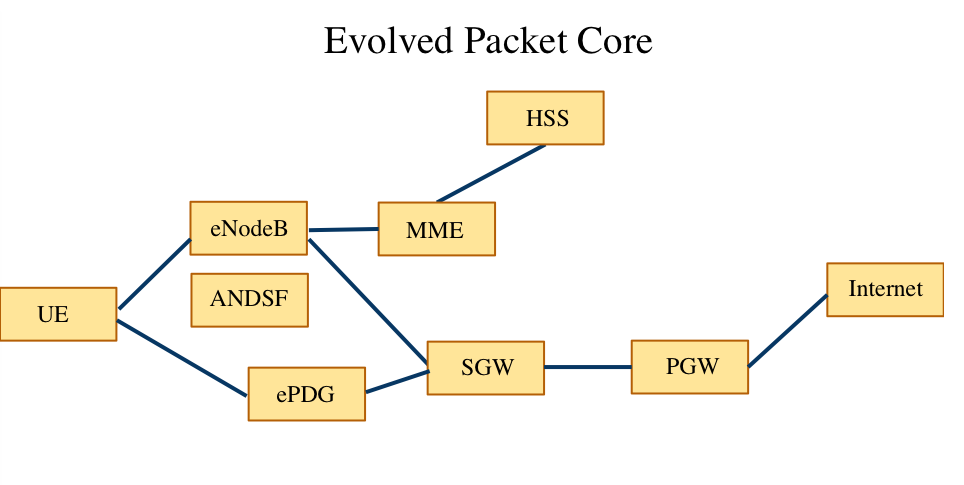
Звонок или сеанс передачи данных, инициированный в зоне покрытия LTE, технически может быть передан без разрыва в сеть 3G (W-CDMA, CDMA2000) или в GSM/GPRS/EDGE. Таким образом, развитие сетей LTE возможно на уже развитых сетях как операторов GSM (в России — операторов «большой тройки»: МТС, Билайн, МегаФон, и региональных операторов «Tele2 Россия» и ОАО «Смартс») так и операторов CDMA (в России — Енисейтелеком, Скайлинк, Сотел ССБ, БайкалВестКом, на Украине — Интертелеком, Пиплнет), что заметно снижает стоимость развертывания сети (в отличие от WiMax сетей).

**SAE** (англ. *System Architecture Evolution* — Эволюция системной архитектуры) это архитектура ядра сети, разработанная консорциумом 3GPP для стандарта беспроводной связи LTE.

SAE является эволюционным продолжением ядра сети GPRS, с некоторыми отличиями:

* **упрощенная архитектура** — архитектура SAE снижает эксплутационные и капитальные расходы. Новая, плоская модель, означает, что потребуется повысить пропускную способность узлов только двух типов (базовых станций и шлюзов), чтобы они справились с трафиком в случае его значительного роста.
* **целиком построена на IP (All IP Network — AIPN)** — Первые концепции 3G были разработаны, с тем, чтобы голос по-прежнему передавался по системе с коммутацией каналов. С тех пор наблюдался переход к IP-сетям. Соответственно архитектура SAE построена на базе IP-сети.
* **обеспечивает большую пропускную способность на сети радиодоступа (radio access network — RAN)** — предполагается, что нисходящий канал (Down Link) будет со скоростью свыше 100 Мбит/с, и основное внимание системы будет сосредоточено мобильности полосы пропускания, от сети потребуется поддерживать гораздо больше уровней данных.
* **обеспечивает меньшую задержку RAN** — с увеличением требуемых уровней взаимодействия и более быстрых ответов, концепция SAE обеспечит уровень задержки в районе 10 мс.
* **поддерживает мобильность между несколькими гетерогенными RAN**, включающим поддержку, как систем типа GPRS, так и не-3GPP систем (например WiMAX)

## Архитектура SAE

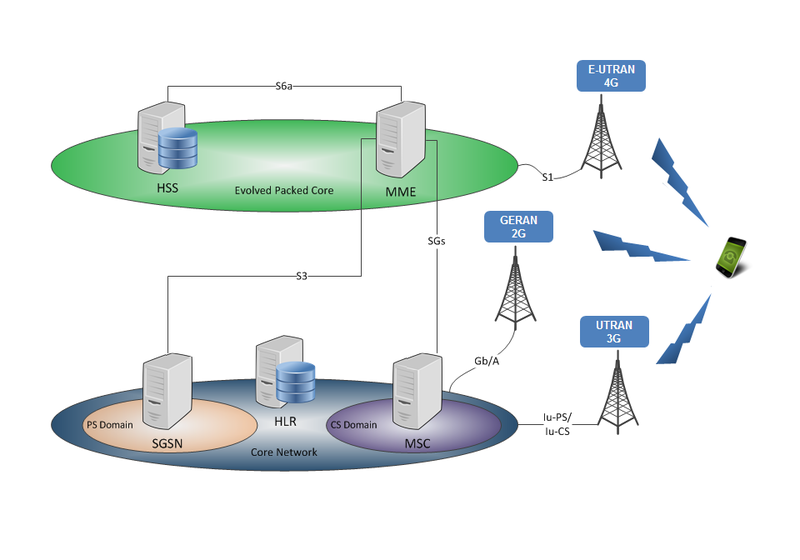


Основным компонентом архитектуры SAE является **Evolved Packet Core** (**EPC**). EPC служит эквивалентом сети GPRS.

Компонентами EPC являются:

* **MME** (Узел Управления Мобильностью — Mobility Management Entity) — это ключевой контролирующий модуль для сети доступа LTE. Он отвечает за процедуры обеспечения мобильности, хэндовера, слежения и пейджинга UE (Пользовательского Устройства — User Equipment). Он участвует в процессах активации/дезактивации сетевых ресурсов и так же отвечает за выбор SGW для UE при начальном подключении и при хэндовере внутри LTE со сменой узла Ядра Сети (Core Network — CN). Он отвечает за аутентификацию пользователя (при взаимодействии c HSS). Сигнализация Слоя Без Доступа (Non-Access Stratum — NAS) оканчивается в MME и данный узел так же отвечает за генерацию и распределение временных идентификаторов для UE. Он проверяет авторизацию UE для доступа к сервис-провайдерам мобильных сетей (Public Land Mobile Network — PLMN) и реализует роуминговые ограничения для UE. MME является заключительной точкой сети для шифрования/защиты целостности сигнализации NAS и отвечает за управление безопасностью. Узаконенный перехват сигнализации так же обеспечивается MME. MME предоставляет плоскость функций контроля для обеспечения мобильности между LTE и сетями доступа 2G/3G через интерфейс S3 установленный к MME от SGSN. MME также соединен интерфейсом S6a с домашним HSS для роуминга UE.
* **SGW** (Обслуживающий Шлюз — Serving Gateway): Предназначен для обработки и маршрутизации пакетных данных поступающих из/в подсистему базовых станций. SGW маршрутизирует и направляет пакеты с пользовательскими данными, в то же время выполняя роль узла управления мобильностью (mobility anchor) для пользовательских данных при хэндовере между базовыми станциями (eNodeB), а также как узел управления мобильностью между сетью LTE и сетями с другими технологиями 3GPP. Когда UE свободен и не занят вызовом, SGW проключает нисходящий канал данных (Down Link — DL) и производит пейджинг, если требуется передать данные по DL в направлении UE. Он управляет и хранит состояния UE (например требования по пропускной способности для IP-сервисов, внутреннюю информацию по сетевой маршрутизации). Он также предоставляет копию пользовательских данных при узаконенном перехвате.
* **PGW** (Пакетный шлюз — Packet Data Network Gateway): Пакетный шлюз обеспечивает соединение от UE к внешним пакетным сетям данных, являясь точкой входа и выхода трафика для UE. UE может иметь одновременно соединение с более чем одним PGW для подключения к нескольким сетям. PGW выполняет функции защиты, фильтрации пакетов для каждого пользователя, поддержку биллинга, узаконенного перехвата и сортирование пакетов. Другая важная роль PGW — являться узлом управления мобильностью между 3GPP и не-3GPP технологиями, такими как WiMAX и 3GPP2 (CDMA 1X и EvDO).
* **PCRF** (Узел выставления счетов абонентам - Policy and Charging Rules Function (*англ.*)): Это - общее название для устройств в рамках SAE EPC, которые отслеживают поток предоставляемых услуг, и обеспечивают тарифную политику. Для приложений, требующих контроль или начисление платы в режиме реального времени, может использоваться дополнительный сетевой элемент под названием Applications Function (AF).

Кардинальные изменения коснулись и ядра сети. В LTE забыли про старый, добрый ОКС7 и перешли на новый протокол — DIAMETER (на базе IP). Все сигнальные интерфейсы между элементами сети работают по протоколу DIAMETER, за исключением legacy 3G элементов, соединения с которыми происходят по SIGTRAN (опят же IP).



## Распределение интеллекта в SAE

Для соблюдения требований к увеличению пропускной способности и уменьшению времени отклика, а также для перехода к all-IP сети, необходимо использовать новый подход к структуре сети.

Ранее, сеть радиодоступа 3G состояла из Node B (базовых станций) и Контроллеров Радиосети (Radio Network Controllers - RNC). Несколько Node B были подключены по принципу "звезда" к RNC, который нес основную нагрузку по управлению радиоресурсом. В свою очередь, RNC были подключены к ядру сети и через него соединялись между собой.

Для обеспечения необходимой функциональности в рамках LTE, в структуре SAE, слой управления сдвигается от ядра к периферии. Управляющие узлы RNC удаляются и управление радиочастотным ресурсом передается базовым станциям. Новый тип базовых станций получил название eNodeB или eNB.

eNB подключаются непосредственно к шлюзу основной сети через новый "интерфейс S1". В дополнение к нему, новые eNB соединяются с соседними eNB по принципу сети через "интерфейс X2". Это обеспечивает гораздо более высокий уровень прямого взаимодействия. Данное подключение, также позволяет направлять многие вызовы напрямую, поскольку большое количество звонков и соединений в сети предназначаются для мобильных устройств в той же или соседних сотах. Новая структура позволяет направлять вызовы по более короткому маршруту и с минимальным использованием ресурса ядра сети.

В дополнение к реализации 1 и 2-го уровней OSI, eNB управляет рядом других функций, которые включают в себя контроль радио ресурсов (включая управление доступом), балансировку нагрузки и управление мобильностью, включая принятие решений о хэндовере для мобильных пользователей или оборудования (UE).

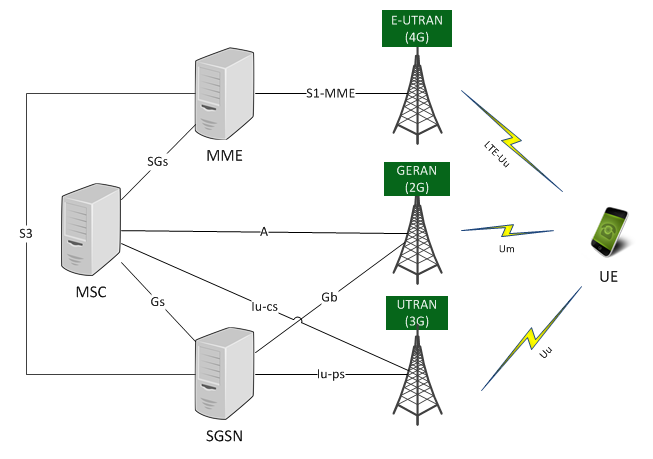
Дополнительные уровни гибкости и функциональности означают, что новые станции eNB являются более сложными, чем станции UMTS или базовые станции предыдущих поколений. Однако новая структура сети SAE позволяет обеспечить производительность гораздо более высокого уровня. В дополнение, гибкость, заложенная в eNB, позволяет им поддержать дальнейшее расширение функциональности для перехода от LTE к LTE Advanced.

## Передача голоса

Сети LTE предназначены для передачи пакетной информации, голоса в этой сети нет в том смысле, в котором мы это понимаем на примере традиционных сетей GSM/UMTS. Но, есть возможность это изменить.

В настоящий момент ведется тестирование и настройка технологии CSFB, которая использует существующий сейчас, традиционный CS (Сircuit switching) домен сетей 2G/3G. Это делается потому, что оригинальная технология передачи голоса в LTE — VoLTE (Voice over LTE), где голос передается уже по IP-сети, используя средства LTE без задействования сетей прошлых поколений, зависима от очень многих решений и разрешений государственного уровня. Для того, чтобы создать условия для совершения звонков с помощью VoLTE, необходимо обеспечить поддержку этого функционала не только сетью, но и пользовательским оборудованием (User Equipment/UE).

#### CSFB – Circuit switch fallback

Упрощенная архитектура EPS-сети для организации CS fallback и передачи SMS-сообщений приведена на рисунке и основана на использовании интерфейса SGs:

###### Особенности/характеристики оборудования поддерживающего CS fallback

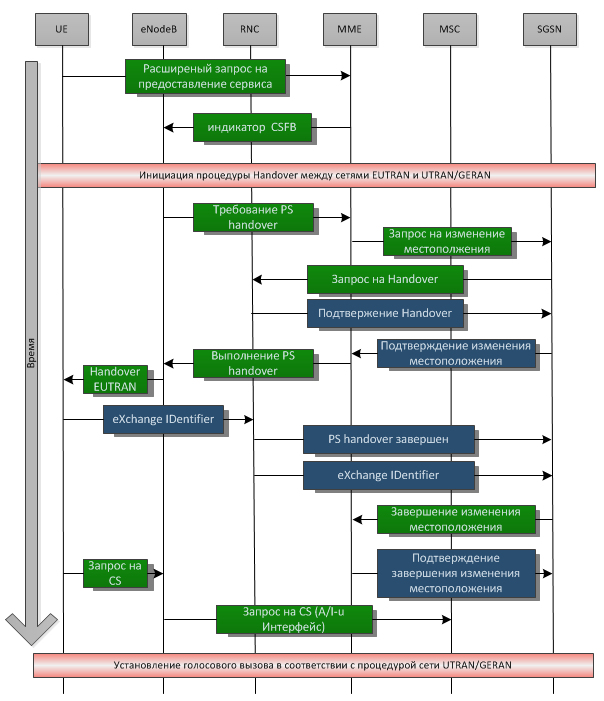
**UE**, естественно, имеет доступ и к E-UTRAN/EPC, и к CS domain через сеть GERAN и/или UTRAN.

**MME** использует LAI и hash-значение, получаемое из IMSI, для определения номера VLR, в случае, если данный LAI обслуживают несколько MSC/VLR, в **SGSN** используется это же hash-значение/функция.

С **MSC** всё понятно, но также возможно расширение функционала CS fallback поддержкой ICS и/или SRVCC.

#### Mobile Originated Call – Абонент звонит из LTE

Что происходит во время совершения вызова абонентом, который находится в сети LTE? Посмотрим на упрощенный call flow (диаграмма обмена сигнальными сообщениями между элементами сетей), который довольно наглядно позволит все объяснить:



###### Рассмотрим базовый сценарий развития событий

Счастливый обладатель телефона с поддержкой LTE идет по улице в зоне покрытия сетей 4G и 3G/2G. В фоновом режиме обновляется почта, Facebook, Twitter и другие сервисы. Решив позвонить, он совершает привычные для себя действия: набирает номер и нажимает кнопку вызова касается того место на экране, где изображена кнопка вызова.

В этот момент генерируется первый *расширенный* запрос (еще 2 года назад сложно было вообразить, что простейший голосовой вызов будет интерпретироваться как расширенный запрос) на предоставление сервиса. MME получает запрос, имея информацию о том, что абонент находится в сети LTE, сообщает об этом eNodeB, чтобы он инициировал процедуру CSFB. Процедура CSFB подразумевает перевод в 2G/3G-сеть, но телефон в это время уже активно использует сеть: получает почту и обновления от сервисов, и прерывать этот процесс нельзя. eNodeB, видя активную передачу данных, принимает решение произвести handover в сеть 3G или 2G. Решение о выборе сети принимается на основании полученных от UE измерений. Таким образом, переход между сетями происходит без разрыва активных сессий передачи данных.

Свое решение eNodeB сообщает MME, и тогда MME уже начинает договариваться с SGSN. Чтобы начать этот процесс, необходимо удостовериться в наличии необходимых ресурсов для данного абонента в SGSN (PFCs, PDP context, APN) и в RNC. Для этого MME передает запрос на изменение местоположения (Update Location) в SGSN. SGSN, в свою очередь, проводит соответствие LTE сервисов (EPS bearer service) не-LTE сервисам (PDP context) и запрашивает выделение ресурсов (PFCs — Packet Flow Context) в RNC. Не обязательно все сервисы будут приняты, в зависимости от загруженности 3G-сети, часть EPS-сервисов может быть отброшена.

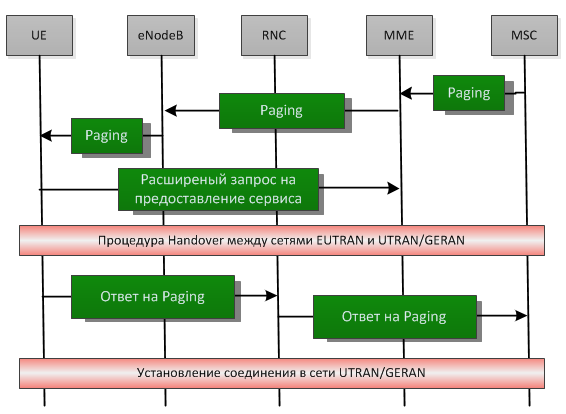
Затем RNC подготавливает так называемый «прозрачный контейнер от источника к получателю», в котором будут данные, как для 3G-сети (Handover Radio Resources), так и для LTE (NAS контейнер). Получив подтверждение о наличии необходимых ресурсов, SGSN сообщает об этом MME, который инициирует процедуру Handover (посылает «прозрачный контейнер» на eNodeB).

eNodeB, получив команду, начинает «переключать» сервисы с MME на SGSN, и вместе с этим посылает команду Handover (с «прозрачным контейнером») на UE. По этой команде UE (смартфон) начинает перестраиваться на радиочасть 3G-сети. Именно для этих целей «прозрачный контейнер» содержит данные для handover как LTE, так и сетей 3G. После перестройки в новую сеть UE посылает сообщение XID (eXchange IDentifier) и в этот же момент возобновляет передачу данных. RNC информирует SGSN об успешном завершении handover, а так же ретранслирует XID на SGSN. После получения подтверждения Update Location начинается высвобождение ресурсов MME и eNodeB.

А далее происходит отработанная годами процедура стандартного голосового вызова в сетях 2G/3G.

#### Mobile Terminated Call – Абоненту звонят в LTE

Входящий вызов в LTE практически ничем не отличается от рассмотренного выше исходящего вызова, за исключением того, что инициатором вызова является не UE, а MSC.



Для начала по SGs-интерфейсу MME принимает paging от MSC с необходимой информацией (IMSI, VLR TMSI, Location Information). В зависимости от настроек paging проходит либо по IMSI, либо по TMSI. В первом случае MME использует IMSI, во втором генерирует из полученных данных S TMSI и передает на eNodeB. Получив paging, смартфон начинает запрашивать радиоресурсы и генерирует расширенный запрос. Как и в предыдущем сценарии, происходит handover, и после него UE отвечает на paging в сети 2G/3G. Голосовое соединение установлено.

Вот так относительно просто можно задействовать legacy-сеть для восполнения голосовых сервисов в сети нового поколения на пути к грядущему VoLTE.

## Технология CSFB имеет несколько недостатков:

- Требует модернизации MME и MSC для сигнализации и SMS;

- Требуется перекрытие зон GERAN/UTRAN и E-UTRAN;

- Увеличение задержки при установлении голосового соединения;

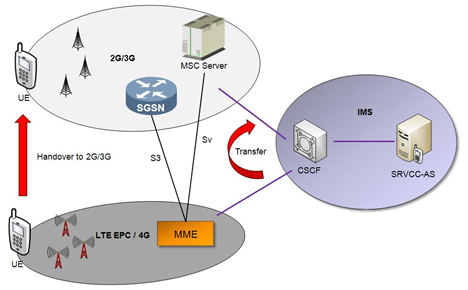
- Снижение скорости передачи данных до скоростей 2,5G/3G;

- Требуется время, чтобы мобильный терминал вернулся в сеть LTE после окончания разговора.

Первым шагом для совершения голосовых вызовов непосредственно в самой сети LTE (VoLTE) является установка платформы IMS (IP Multimedia Subsystem). IMS представляет собой программно-аппаратный комплекс, который является ключевым компонентом практически всех IP-сетей следующего поколения.

**SRVCC (Voice over LTE).**

Голосовые вызовы, инициируемые в сети LTE, осуществляются в LTE сети по IP на базе IMS-платформы (VoLTE). В случае потери LTE покрытия голосовой вызов перенаправляется в 2G/3G сеть коммутации каналов (CS-voice). Для этого необходима активация функционала Single Radio Voice Call Continuity,



Обслуживание голосовых вызовов происходит в сети LTE за счет передачи пакетов данных голосового сигнала через пакетные каналы (Voice over IP).

Мобильность голосового сервиса реализуется посредством функционала SRVCC-процедуры хэндовера с выбором соты назначения из сети LTE (PS-сервис) в 2G/3G (CS-сервис), в случае деградации радиопокрытия LTE.

Применение технологии SRVCC позволяет сократить время установления голосового соединения в среднем 1 секунда. Более того, технология позволяет улучшить качество голосового сервиса на 10-15%, чем в сети 2G/3G.

Для реализации этого сервиса сеть должна поддерживать сетевую архитектуру описанную начиная с 3GPP Release 8. Различают несколько видов SRVCC handover – CS\_Only и CS\_and\_PS. Данный параметр настраивается в радио сети, и передаётся в изначальном запросе на handover, что определяет дальнейшие действия MME Технология SRVCC должна поддерживаться мобильными устройствами.

Основными трудностями внедрения данной технологии является:

- Высокие затраты на установку IMS платформы

- Отсутствие качественного LTE покрытия

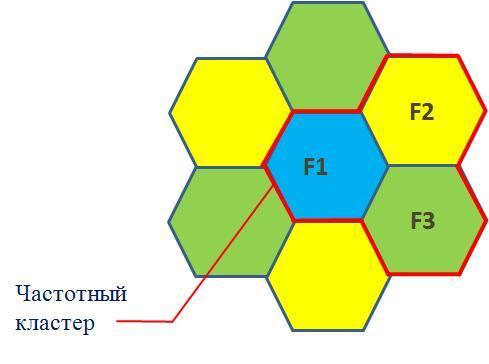
- Малое количество устройств с поддержкой данной функции

## Об ОТТ сервисах

Дальнейшему внедрению услуг VoLTE может препятствовать оказание голосовых ОТТ-услуг. На сегодняшний день существует и используется способ голосовой связи посредством OTT (Over-the-Top) сервисов, таких как Skype, Google Voice, WhatsApp, Viber и т.д. Сеть передачи данных, в основе которой лежит IP, дает удобный транспорт для совершенно разных услуг и выводит управление ими за пределы зоны ответственности оператора к самим пользователям. Но такой способ не удовлетворяет пользователей, так как эти сервисы не гарантируют стабильную, качественную работу. Дело в том, что в OTT сервисах используется тип трафика который имеет более низкий приоритет, чем тип трафика при VoLTE.

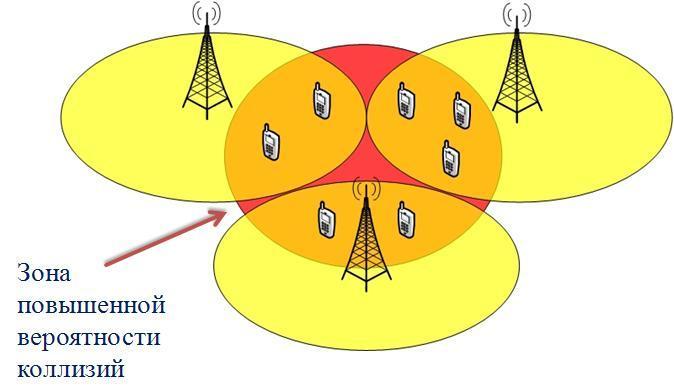
## Межсотовая интерференция

Как вообще работает LTE сеть в условиях полного отсутствия частотно-территориального планирования (Frequency Reuse Factor=1!)? Рассмотрим сети постарше, допустим GSM (см. ниже):

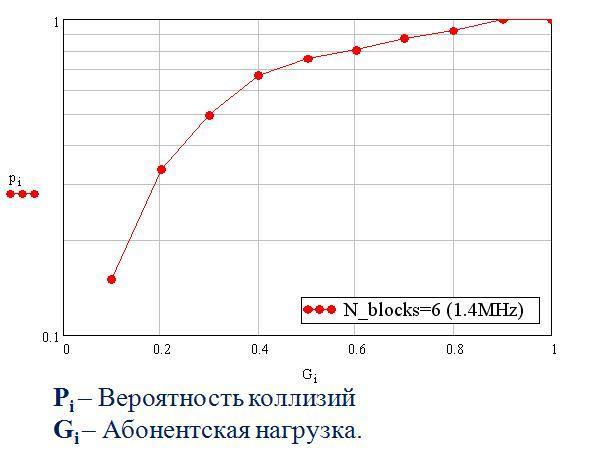


Весь частотный диапазон делился на поддиапазоны, и главное правило планирования заключалось в том, чтобы в соседних сотах использовались разные частотные полосы, в противном случае, сигналы соседних сот были бы интерферирующими, мешали бы счастливой жизни друг друга. В UMTS (WCDMA) все было несколько сложнее — все базовые станции (NodeB) использовали один и тот же частотно-временной ресурс и для разделения сигналов от разных сот, или сигналов от разных абонентов внутри одной соты применялось скремблирование разного типа ортогональными или псевдоортогональными последовательностями.

Так или иначе — проблема межсотовой интерференции (ICI-Inter-cell Interference) в сетях GSM и UMTS стояла неостро… Что же мы видим в LTE? Мало того, что во всех сотах используется одна и та же полоса частот, так и скремблирование сигналов ортогональными последовательностями (в общем случае) отсутствует. Что это значит? Если две соседние БСки (eNB) выделяют своим абонентам под передачу данных ресурсные блоки в одной и той же полосе частот и в одно и то же время, то можно с определенной долей вероятности утверждать, что эти абоненты будут мешать друг другу, будут интерферировать. Самая неприятная ситуация будет наблюдаться на краях сот:



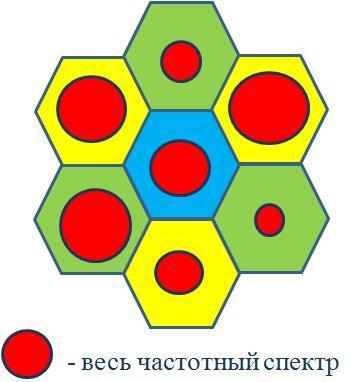
На вероятность коллизии в данном случае (вероятность искажения пакета из-за одновременного выделения двумя или более базовыми станциями одного и того же ресурса пользователям), очевидно, будут влиять два фактора: 1) удаленность абонентов друг от друга, иначе — их близость к БС (если абоненты находятся близко к БС, то включается механизм управления мощностью (Power Control), который скорее всего вынудит телефон понизить уровень передаваемой мощности, как следсвие, снизится общий уровень интерференции между сотами). 2) нагрузка в соте (тоже достаточно очевидный фактор — чем выше нагрузка, тем больше вероятность одновременного выделения абонентам на краях соты одного и того же ресурсного блока). Если сымитировать работу такого примитивного планировщика, неосведомленного о нагрузке на соседнии соты и пр., и вывести вероятность коллизии между пакетами в разных сотах (по сути, это косвенное отражение уровня межсотовой интерференции), то получится такая зависимость:



За единицу или максимум нагрузки принимается ситуация, когда все блоки частотно-временного ресурса распределены. Сказать, что такие значения вероятности искажений пакетов огромны — это ничего не сказать. Это вопиюще плохая интерференционная картина. И, разумеется, вряд ли бы кто-то выпустил LTE с такими характеристиками в свет.

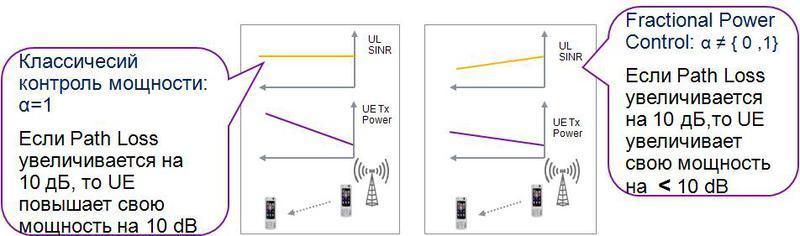
Итак, что сделано в LTE, чтобы избежать этой катастрофической интерференции между сотами и не прибегнуть при этом к повторному переиспользованию частот.

Во-первых, в LTE работает механизм под названием **ICIC (Inter-Cell Interference Coordination — Координация межсотовой интерференции)**… Интересная штука, надо сказать. Ее детальное описание со всеми выкладками можно найти в замечательной книжке, приведенной в конце этой статьи, в разделе 12.5, кому интересно. Смысл фитчи в том, что соседние eNB (БСки) передают по X2 интерфейсу информацию о своей загрузке в виде Overload Indicator (OI). Таким образом, они фактически имеют возможность договориться между собой кто из них какой поддиапазон (subband) в какой момент времени будет использовать. Выглядеть частотно-территориальное распределение в этом случае будет примерно так:



То есть, абонентам, находящимся ближе к антенне, eNB может отдавать любые ресурсные блоки, а тем кто подальше — в зависимости от OI-индикатора. Это ни в коем случае не классическое переиспользование частот. Это адаптивное распределение ресурсов, подстраивающееся под нагрузку на соседние соты и это основной способ уменьшения интерференции между сотами (уменьшения — но не полного устранения, разумеется).

Помимо таких механизмов направленного действия, в LTE предусмотренны косвенные методы снижения интерференции. Например, Fractional Power Control. Если классический контроль мощности был нацелен на полную компенсацию потерь сигнала во время распространения (PathLoss compensation), то частичный контроль мощности означает частичную компенсацию таковых потерь.



Параметр, задающий значение коэффициента для компенсации Path Loss, называется в стандарте Альфа (принимает значения от 0 до 1). Как это работает: значение альфа, равное 0,8 (80 %- компенсация потерь сигнала), позволяет снизить уровень межсотовой интерференции на 10-20%! При этом абоненты на краях соты не испытывают заметных проблем, вызванных неполной компенсацией Path Loss.

Существует еще множество параметров, которые можно подстраивать, чтобы соты меньше интерферировали, но ICIC и Fractional Power Control — это, пожалуй, два самых мощных механизма.

## Downlink канал и множественный доступ

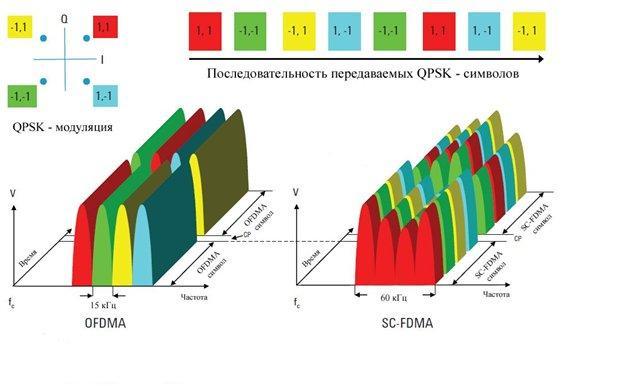
Особенностью линии «вниз» сети E-UTRAN является использование технологии множественного доступа SC-FDMA (Single Carrier – Frequency Division Multiple Access) c одной несущей частотой и средней мощностью передачи PAPR (Peak-to-Average Power Ratio). Исключение взаимного влияния пользователей достигается введением циклических префиксов и использованием эффективных эквалайзеров в приемных устройствах. Интервал времени передачи TTI в линии «вверх» сети E-UTRAN соответствует TTI в линии «вниз» и равен 0.5 мс. Возможно использование увеличенного TTI для специальных типов соединений (услуг). Основная конфигурация антенн линии «вверх» при использовании MIMO предполагает использование двух передающих антенн на мобильном терминале и двух приемных антенн на базовой станции.

SC-FDMA представляет собой гибридную схему передачи, которая сочетает низкие значения PAR, присущие системам с одной несущей, таким как GSM и CDMA, с большой длительностью символа и гибким распределением частот OFDM. Принципы генерации сигнала SC-FDMA показаны на рисунке 1, который является фрагментом одного из рисунков отчета 3GPP TR 25.814 об исследовании физического уровня LTE.



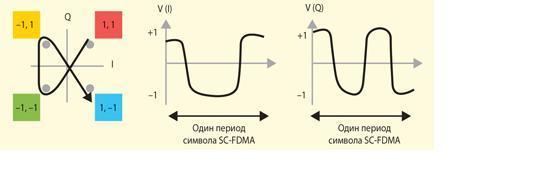


Прохождение сигнала в восходящем канале связи (Uplink).

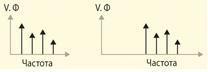


Сравнение передачи серии символов данных QPSK в OFDMA и SC-FDMA

В левой части рисунка 1 символы данных представлены во временной области. Символы преобразуются в частотную область с помощью быстрого преобразования Фурье и затем, в частотной области, они распределяются в нужные места общего спектра несущей. Затем их требуется снова преобразовать во временную область, чтобы перед передачей добавить к ним циклический префикс.



Создание символа SC-FDMA во временной области

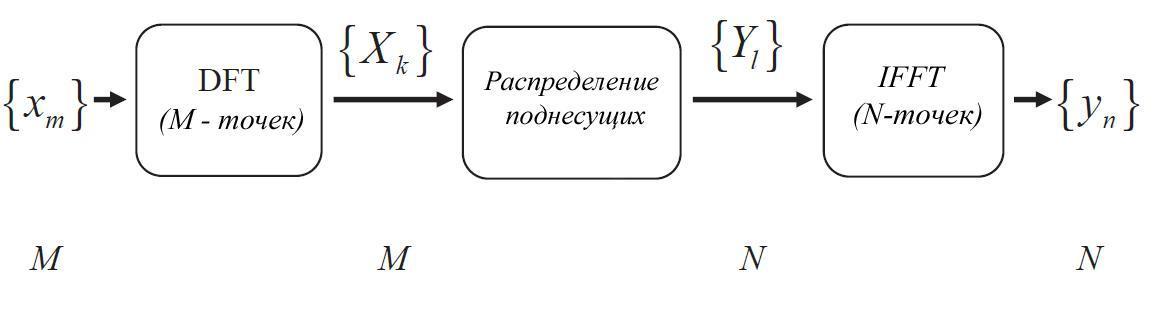


Представление символа SC-FDMA в полосе модулирующего сигнала и со сдвигом по частоте.

В продолжение графического сравнения OFDMA и SC-FDMA на рисунках показан детальный процесс генерации сигнала SC-FDMA. Сначала создается представление последовательности символа данных во временной области. В данном примере с четырьмя поднесущими для генерации одного символа SC-FDMA требуются четыре символа данных. Используя первые четыре цветных символа QPSK, процесс создает один символ SC-FDMA во временной области, рассчитывая траекторию, переходящую от одного символа данных QPSK к другому. Это делается со скоростью в M раз выше скорости символов SC-FDMA, так что в результате один символ SC-FDMA содержит M последовательных символов данных QPSK. Чтобы не усложнять рассмотрение, мы не будем обсуждать фильтрацию переходов между символами, хотя в любой реальной схеме такая фильтрация обязательно присутствует.

В частотной и временной областях показано, как OFDMA и SC-FDMA передают последовательность из восьми символов QPSK. В этом упрощенном примере число поднесущих (M) было сокращено до четырех. Для OFDMA четыре (M) символа обрабатываются параллельно, причем каждый из них модулируется собственной поднесущей с соответствующей фазой QPSK. Каждый символ данных занимает полосу 15 кГц на время передачи одного символа OFDMA, которое равно 66,7 мкс. В начале следующего символа OFDMA вставляется защитный интервал, содержащий циклический префикс (CP). CP представляет собой копию конца символа, добавленную к началу символа. Благодаря параллельной передаче, символы данных имеют ту же длину, что и символы OFDMA.

В случае SC-FDMA символы данных передаются последовательно. Поскольку в данном примере используются четыре поднесущих, за один период символа SC-FDMA передаются четыре символа данных. Период символа SC-FDMA имеет ту же длину, что и символ OFDMA, т.е. 66,7 мкс, но благодаря последовательной передаче символы данных получаются короче, т.е. равными 66,7/M мкс. В связи с повышением скорости следования символов для их передачи требуется более широкая полоса. В результате каждый символ занимает в спектре 60 кГц, а не 15 кГц, как было в случае более медленных символов, используемых в OFDMA. После передачи четырех символов данных вставляется CP.

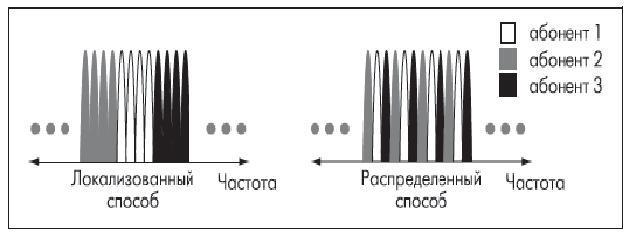


Сама процедура формирования SC-FDMA-сигнала отличается от схемы OFDMA. После канального кодирования, скремблирования и формирования модуляционных символов они группируются в блоки по М символов – субсимволов SC-FDMA. Очевидно, что непосредственно отнести их на поднесущие с шагом 15 кГц невозможно – требуется в

N раз более высокая частота, где N – это число доступных для передачи поднесущих. Поэтому, сформировав группы по М модуляционных символов (М < N), их подвергают М-точечному дискретному Фурье-преобразованию (ДПФ), т.е. формируют аналоговый сигнал. А уже затем с помощью стандартной процедуры обратного N-точечного Фурье-преобразования синтезируют сигнал, соответствующий независимой модуляции каждой поднесущей, добавляют циклический префикс и генерируют выходной ВЧ-сигнал.

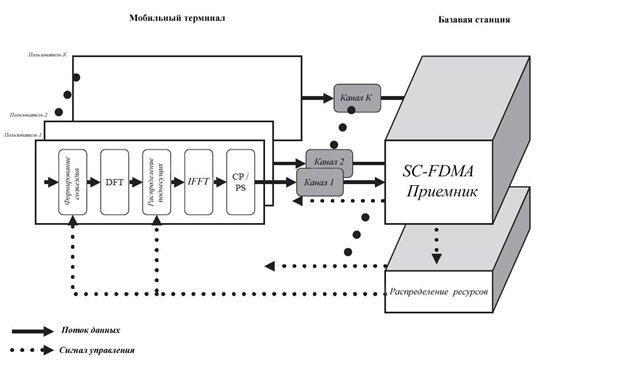
После создания IQ-представления одного символа SC-FDMA во временной области следующим шагом является представление его в частотной области с помощью дискретного преобразования Фурье (DFT; см. рис. 4). Частота дискретизации DFT выбирается таким образом, чтобы форма одного символа SC-FDMA во временной области полностью представлялась M бинами DFT, отстоящими друг от друга на 15 кГц, причем каждый бин представляет одну поднесущую с постоянной амплитудой и фазой в течение одного периода символа SC-FDMA равного 66,7 мкс. При этом всегда существует однозначное соответствие между числом символов данных, передаваемых за один период символа SC-FDMA, и числом создаваемых бинов DFT, которое, в свою очередь, равно числу занимаемых поднесущих. Это достаточно логично: с ростом числа символов данных, передаваемых за один период SC-FDMA, сигнал во временной области изменяется быстрее, что приводит к расширению полосы и, следовательно, требует большего числа бинов DFT для полного представления сигнала в частотной области.

Дискретное преобразование Фурье по M- точкам.



Способы распределения поднесущих в SC-FDMA

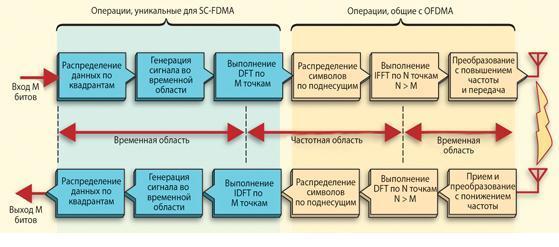
При формировании группового сигнала в линии «вверх» для каждого терминала решается, какая часть поднесущих используется (заполняется данными), а какая нет (заполняется «нулями»)



Распределение ресурсов, в зависимости от затухания в каналах.

Присваивает поднесущих для пользователей идет в соответствии с частотной характеристикой каналов каждого пользователя.

Теперь самое время задать вопрос: «Как же может SC-FDMA сохранить стойкость к многолучевому распространению при столь коротких символах данных?». В OFDMA модулирующие символы данных остаются постоянными в течение периода символа OFDMA равного 66,7 мкс, тогда как символ SC-FDMA меняется со временем, поскольку содержит M коротких символов данных. Стойкость к многолучевому распространению процесса демодуляции OFDMA обусловлена большой длиной символов данных, которые накладываются непосредственно на отдельные поднесущие. К счастью, стойкость к разбросу задержки обусловлена именно постоянной природой каждой поднесущей, а не постоянством символов данных. Как показано выше, DFT изменяющегося во времени символа SC-FDMA создает набор бинов DFT, постоянных в течение символа SC-FDMA, несмотря на то, что модулирующие символы данных при этом изменяются. В этом и заключается основное свойство процесса DFT, что изменяющийся во времени символ SC-FDMA, состоящий из M последовательных символов данных, представляется в частотной области M не меняющимися во времени поднесущими. Таким образом, даже SC-FDMA с присущими ему короткими символами данных обладает достаточной стойкостью к многолучевому распространению. Теперь для завершения генерации сигнала SC-FDMA выполняются те же операции, что и для OFDMA. Обратное БПФ преобразует смещенный по частоте сигнал во временную область, а затем добавление CP обеспечивает свойственную OFDMA фундаментальную стойкость к многолучевому распространению.



**Взаимосвязь модуляции OFDMA и SC-FDMA.**

Оранжевые блоки показывают обработку OFDMA, а синие блоки представляют дополнительную обработку во временной области, необходимую для SC-FDMA. Главное, что следует отметить, это то, что сигнал, преобразованный из частотной области обратно во временную область, представляет собой ни что иное, как смещенную по частоте версию последовательности символов QPSK. Данный пример демонстрирует основную причину создания SC-FDMA, а именно, PAR конечного сигнала не превышает PAR исходных символов данных, которые в данном случае являются символами QPSK. Это существенно отличается от OFDMA, где параллельная передача тех же символов QPSK создает статистические пики, очень похожие на Гауссовский шум, которые значительно превышают PAR исходных символов данных. Ограничение PAR с помощью SC-FDMA существенно снижает потребность в том, чтобы мобильное устройство работало с высокими пиками мощности. Это снижает и затраты, и энергопотребление.

## LTE-A

В первом квартале 2011 года 3GPP выпустила первую версию протокола LTE-Advanced (LTE-A): LTE-A Release10. LTE-A была получена посредством развития технологии LTE с целью соответствия возрастающим требованиям IMT Advanced, — четвертого поколения мобильных систем коммуникации.

Технология LTE-A значительно увеличивает пиковые значения скорости ПД, пиковую спектральную эффективность, значения средней скорости ПД, среднюю спектральную эффективность и производительность абонентов на границе ячейки покрытия. Она улучшает эффективность сети по всей сети и будет основным направлением развития мобильных коммуникаций в будущем, находясь на гребне волны новой эры мобильной широкополосной передачи данных (МШПД).

Количество мобильных абонентов и абонентов мобильной ШПД продолжает увеличиваться очень быстро. Среднегодовые темпы роста количества абонентов за 2007–2011 годы составили 104%. Агентство Infonetics подсчитало, что количество абонентов мобильных услуг в мире достигло 5,2 млрд. в 2011 году, количество абонентов мобильной ШПД превысило 5 млрд., а рост трафика в расчете на абонента превысит 50% в последующие 10 лет. При этом трафик мобильной сети вырастет в ошеломляющие 500 раз. Все это обуславливает внедрение LTE-A для обеспечения требований по передаче огромных объемов информации по сети большой емкости.

**Ключевые технологии LTE-A**

Технология LTE-A расширяет и усиливает базовую платформу технологии LTE. В частности, это касается более гибкого и эффективного использования частотных ресурсов, более высокой спектральной эффективности, более простой и оптимизированной архитектуры сети и способности снизить совокупные затраты (TCO) и предоставлять больше услуг. Технология LTE-A обратно совместима с LTE и представляет собой плавную эволюцию последней. Технология LTE-A должна поддерживать полосу частот до 100 MГц, пиковую скорость на даунлинке до 1 Гбит/с со спектральной эффективностью, улучшенной до 30 бит/с на 1 Гц, и пиковую скорость на аплинке до 500 Мбит/с со спектральной эффективностью, улучшенной до 15 бит/с на 1 Гц и расширение MIMO на аплинке и даунлинке до 8х8 и 4х4 соответственно.

Ключевые технологии, позволяющие LTE-A реализовать эти требования, это:

• объединение несущих (Carrier Aggregation СА);

• усиление MIMO (Enhanced MIMO);

• скоординированный многоточечный прием/передача (Coordinated Multipoint Tx/Rx- СоМР);

• неоднородная сеть (Heterogeneous Network- HetNet);

• самоорганизующаяся сеть (Self Organization Network (SON).

Рассмотрим их более подробно.

**Объединение несущих (CA)**

Чтобы выполнить требования по пиковой скорости — аплинк до 500 Мбит/с и даунлинк до 1 Гбит/с — LTE-A должен поддерживать работу с полосой частот до 100 МГц. Однако, почти невозможно найти столь широкую полосу частот в доступных частотных ресурсах на сегодняшний день. Поэтому LTE-A использует технологию объединения несущих (CA) для полного использования частотных ресурсов, разбросанных в разных частотных диапазонах. Это позволяет не только использовать имеющиеся частотные ресурсы по максимуму, но и гарантирует обратную совместимость с LTE.

Наибольшая полоса частот, используемая в настоящий момент технологией LTE, — 20 МГц. Технология же LTE-A объединяет несколько несущих в разных частотных диапазонах, совместимых с LTE для поддержки суммарной полосы частот до 100 MГц. LTE-A использует три формы объединения несущих — непрерывный CA в диапазоне, прерывающийся CA в диапазоне и прерывающийся CA вне диапазона — для объединения нескольких непрерывных и прерывающихся частей несущих в одном или нескольких диапазонах. При заданной асимметричности трафика на аплинке и даунлинке LTE-A может также объединять асимметричные несущие, поскольку при типичном использовании полоса частот для даунлинка больше полосы частот аплинка. Технология CA может не только значительно увеличить утилизацию частотных ресурсов, но также помогает операторам гибко комбинировать неширокие полосы частот в разных диапазонах для увеличения пиковой скорости абонентов и общей пропускной способности сети. CA не предполагает каких-либо дополнительных требований к принимающей способности терминалов. Поэтому терминалы LTE-A со способностью работать с полосой частот свыше 20 МГц могут принимать несколько частей несущих одновременно, в то время как терминалы LTE Rel.8 могут принимать только одну несущую частоту.

**Усиление MIMO (Enhanced MIMO)**

Учитывая то, что новые частотные ресурсы становятся все более недоступными, увеличение емкости частотного канала посредством использования мультиантенн широко применяется во множестве стандартов связи. Примечательно, что это ключевая технология увеличения пиковой и средней спектральной эффективности LTE-A. Технология LTE Rel.8 поддерживает передачу на даунлинке посредством одной, двух или четырех антенн, две или четыре антенны на прием на терминальном оборудовании и максимум до четырех уровней передачи на даунлинке. На аплинке LTE Rel.8 поддерживает одну передающую антенну на терминале и максимум до 4 принимающих антенн на базовой станции. Режим мультиантенной передачи в технологии LTE Rel.8 включает в себя незамкнутый MIMO, замкнутый MIMO, формирование луча направленности и диверсифицированную передачу.

В дополнение к однопользовательскому MIMO LTE также использует граничную мультиантенную передачу — мультипользовательское MIMO — для увеличения спектральной эффективности, что позволяет нескольким пользователям использовать один ресурс передачи посредством пространственного разделения. На базе LTE Rel.8, LTE-A поддерживает максимум 4 передающие антенны на аплинке. Если совместный физический канал аплинка (PUSC) принимает MIMO для одного пользователя, LTE-A может поддерживать до двух кодовых потоков и четыре уровня передачи. Также PUSC может улучшить качество передачи и покрытия для аплинка, контроль информации через разнос передачи. LTE-A поддерживает до восьми передающих антенн на даунлинк и может передавать два кодовых потока и максимум до восьми уровней передачи. Это еще больше увеличивает пропускную способность и спектральную эффективность передачи на аплинке и даунлинке. На даунлинке LTE-A поддерживает динамическое переключение между однопользовательским и мультипользовательским MIMO, что увеличивает производительность даунлинка мультипользовательского МIMO посредством передачи информации о состоянии усиленного канала и нового дизайна кодовой книги. Технология мультиантенн LTE-A увеличивает пиковую и среднюю спектральную эффективность и значительно усиливает емкость и покрытие для улучшения производительности сети.

**CoMP**

CoMP позволяет пользователям на краю ячейки покрытия координировать и одновременно получать и отправлять сигналы пользователям мультиячеек. Производительность даунлинка может быть значительно улучшена, если сигналы, передаваемые из мультиячеек, скоординированы, чтобы предотвратить взаимную интерференцию. На аплинке сигналы мультиячеек принимаются и комбинируются. Если мультиячейки скоординированы и распределены на очередь прием/передачи, взаимная интерференция внутри ячеек может быть снижена и отношение сигнал/шум принимаемого сигнала может увеличиться. Базируясь на отношении между ячейками, которые необходимо скоординировать, CoMP подразделяется на два основных режима: СоМР внутри сайта, СоМР между сайтами.

CoMP внутри сайта охватывает координацию на одном сайте. Поскольку нет никаких ограничений на емкость транспортной сети, большие объемы информации могут обмениваться между мультиячейками на одном сайте.

CoMP между сайтами охватывает координацию между несколькими сайтами и предъявляет существенно большие требования к емкости транспортной сети и задержкам прохождения сигнала.

Сейчас производительность CoMP между сайтами ограничена емкостью транспортного канала и задержками. CoMP включает СоМР передачи на даунлинке и СоМР приема на аплинке.

CoMP приема на аплинке увеличивает пропускную способность для пользователя на краю ячейки посредством координирования мультиячеек. СоМР передачи на даунлинке применяет две формы взаимодействия — совместную обработку и совместную диспетчеризацию/формирование луча направленности, в зависимости от того — были ли данные об услуге получены на нескольких точках координации.

Совместная обработка применяется, когда множество ячеек координируются и действуют вместе как единая виртуальная ячейка для обслуживания терминала. Это обычно позволяет получить лучший коэффициент усиления передачи, но предъявляет более высокие требования к емкости транспортной сети и задержкам. Совместная диспетчеризация/формирование луча направленности сигнала значительно улучшает объем информацией между несколькими ячейками и координирует соответствующее планирование и разнос передачи для минимизации взаимной интерференции между ячейками. Терминалы должны измерять сигнал каналов от разных ячеек и передавать ответный сигнал, включая ожидаемый вектор предварительного кодирования от обслуживающей ячейки и вектор предварительного кодирования интерференции от соседних ячеек, которые создают наиболее сильную интерференцию. Координация планировщиков от нескольких соседствующих ячеек помогает каждой ячейке снизить интерференцию на соседние ячейки при передаче сигнала. Это гарантирует силу сигнала, ожидаемую пользователем ячейки.

CoMP — ключевая технология LTE-A, которая эффективно увеличивает среднюю емкость ячеек и отношение сигнал/шум для пользователей на краю зоны покрытия ячейки. Хотя CoMP повышает сложность системы, те преимущества в емкости и покрытии сети, которые она дает, значительно перевешивают недостатки.

**Неоднородная сеть HetNet**

Статистика показывает, что от 80 до 90% трафика в сетях будущего будет производиться в закрытых помещениях и хотспотах. Важность покрытия сети внутри помещений, важность низкоскоростных сетей и покрытие в хотспотах будут постоянно расти в эру мобильного Интернета, требуя от операторов использовать новые технологии для улучшения удовлетворенности абонентов от использования услуг традиционных мобильных сетей в хотспотах. В традиционной сети с макроячейками операторы могут использовать больше частотного ресурса или добавить базовую станцию для увеличения емкости сети. В качестве альтернативы они могут установить большее количество антенн на базовую станцию для использования технологии advanced MIMO. Эти меры увеличивают финансовые затраты и сложность внедрения, сильно ограничивая потенциал эволюции производительности сети с традиционными макроячейками. Технология HetNet значительно увеличивает пропускную способность сети и общую емкость посредством распределения маломощных базовых станций в зонах покрытия макробазовых станций для формирования разнородной системы с различным типом узлов, предлагающих одинаковое покрытие.

Маломощные базовые станции включают в себя базовые станции семейства: micro, pico, удаленная радиоголовка (RRH), relay и femtocell. Увеличение количества маленьких, маломощных базовых станций дешевле, они гибкие в применении и эффективно увеличивают емкость сети. Маленькие станции не только разгружают хотспоты макро БТС, но и улучшают слепые зоны покрытия макробазовых станций.

Ключевая особенность HetNet — совместное использование макробазовых станций и микробазовых станций, особенно в условиях координации интерференции и совместимости.