Лекция 3.

3.1 Виртуальные локальные сети VLAN

3.1.1 Потребность в применении VLAN

Эта потребность возникла практически сразу же после появления первых коммутаторов Ethernet. Преимущества коммутаторов по сравнению с хабами нами уже рассматривалась и поэтому естественным было желание строить сегменты Ethernet сразу на базе коммутаторов. Но стоимость первых коммутаторов Ethernet была довольно высокой (на порядок выше стоимости хабов и в пару раз выше стоимости средних персональных компьютеров той поры). При этом стоимость одного коммутатора с достаточно большим количеством портов была существенно ниже, чем стоимость двух коммутаторов с половинным числом портов (не говоря уж о большем числе коммутаторов с меньшим числом портов).

Поэтому сразу же возникла потребность при использовании одного большого коммутатора с подключенными к его портам подсетями и индивидуальными компьютерами портов конкурирующих подразделений разбить множество портов коммутатора на группы портов, используемых для подключения компьютеров различных подразделений, с обеспечением взаимной изоляции портов различных групп.

Взаимная изоляция групп портов означает полную невозможность обмена трафиком между портами различных групп. Такой обмен возможен лишь через сетевые устройства более высокого уровня (маршрутизаторы), обеспечивающие развитые возможности фильтрации трафика между подсетями. Естественно, что при такой организации каждая из изолированных групп должна использовать один из своих портов для подключения к маршрутизатору, как это показано на рис. 1.

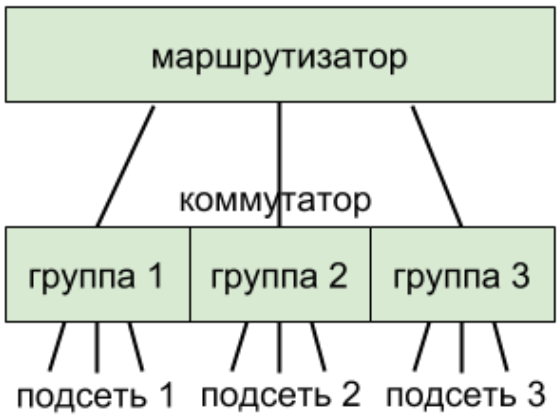

Рис. 1. Организации взаимодействия изолированных групп портов

Рассмотренная потребность была вскоре реализована. При ее реализации изолированные группы портов получили название виртуальных ЛВС (LAN) или VLAN.

Однако с началом применения древовидных структур коммутаторов возникла необходимость в применении VLAN, “пронизывающих” структуру взаимосвязанных коммутаторов, как это показано на рис. 2.

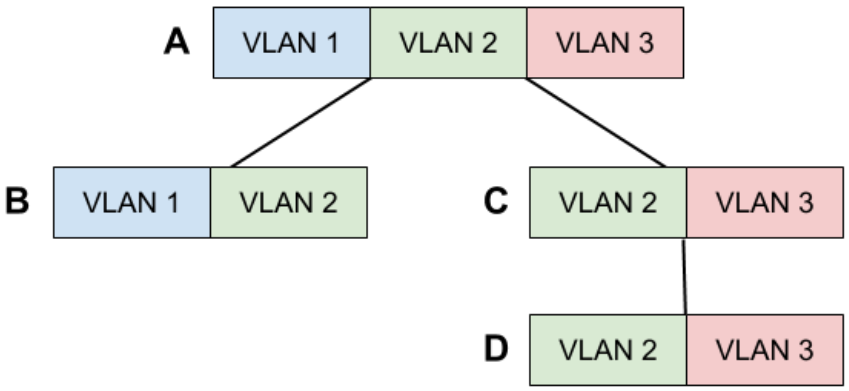

Рис. 2. Пример 3-х VLAN, “пронизывающих” дерево коммутаторов

Естественно, что механизмы реализации VLAN были вскоре расширены для обеспечения возможности реализации такой расширенной потребности.

3.1.2 Определение VLAN и простые следствия из него

Определение: VLAN - это совокупность подмножеств портов на группе взаимосвязанных коммутаторов сети канального уровня, полностью изолированная по трафику от не входящих в эту совокупность других портов коммутаторов сети. Изоляция выполняется для всех типов пакетов: обычных, широковещательных, BPDU.

Из этого определения непосредственно выводятся три простых следствия:

1. В каждой из VLAN за счет исключения возможности обмена между нею и другими VLAN пакетами BPDU обеспечивается независимое построение остовых деревьев этих VLAN средствами протокола STP.
2. Взаимная изоляция VLAN обеспечивает их взаимную информационную безопасность. Всем специалистам в области построения коммутируемых сетей Ethernet хорошо известно простое утверждение: “VLAN не взламываются”. Это значит, что не известны методы “проникновения в” и “прослушивания трафика” любой VLAN из других VLAN, построенной на базе коммутируемых сетей канального (2-го) уровня. Именно поэтому VLAN’ы иногда называют L2 VPN (Layer 2 Virtual Private Network - виртуальная частная сеть уровня 2).
3. Изоляция VLAN от стороннего широковещательного трафика повышает скорость работы в каждой из изолированных подсетей

3.1.3. Механизмы создания VLAN.

Рассмотрим основные способы “отделения” VLAN друг от друга. К ним относятся:

- Группировка портов
- Группировка MAC-адресов
- Добавление к кадрам меток VLAN
-

Группировка портов является самым простым способом разделения VLAN. Суть этого способа состоит в том, что каждый порт коммутатора помечается номером VLAN, к которой относится этот порт. Тогда при передаче каждого кадра коммутатор проверяет, принадлежит ли получатель той же VLAN, что и отправитель. Если да, то кадр направляется по указанному MAC-адресу, иначе кадр выбрасывается.

Этот способ прост и удобен для сетевого администратора. Но этот способ обладает одним серьезным недостатком. Он вызван тем, что при передаче кадра от одного коммутатора к другому (а получатель кадра может быть подключен не к тому же коммутатору, что и отправитель) информация о принадлежности источника к определенной VLAN никак не передается.Поэтому для корректного разделения VLAN необходимо связать “фрагменты” VLAN, расположенные на каждой паре соседних коммутаторов отдельным каналом, не используемым другими VLAN. При сколь либо большом количестве VLAN (а в большой сети их могут быть сотни) возникает проблема

нехватки числа портов коммутатора. Поэтому на практике этот способ используется в сочетании с третьим из указанных выше способов.

Группировка MAC-адресов. При использовании этого способа все MAC-адреса одной сети канального уровня помечаются номерами включающих их VLAN. Этот способ свободен от недостатков предыдущего. Но он требует большого объема кропотливой работы сетевого администратора как при проведении начальной разметки так и при ее изменениях, выполняемых при замене, добавлению и удалению компьютеров (их сетевых карт) размечаемой сети.

Добавление к кадрам меток VLAN. Этот способ (протокол IEEE 802.1q) может применяться только на каналах, связывающих коммутаторы друг с другом. При передаче пакета по такому каналу, который должен быть сконфигурирован как транковый (см. ниже) в заголовок кадра добавляется специальное поле, называемое меткой VLAN и содержащее, в частности, значение номера VLAN. При получении такого расширенного кадра коммутатором получателя кадра этот коммутатор “знает” из какой VLAN пришел кадр и может сравнить ее номер с номером VLAN получателя. Если они совпадают, из кадра удаляется метка VLAN и он направляется получателю.

Важное дополнение к возможностям, обеспечиваемым протоколом IEEE 801.q обеспечивает протокол IEEE 801.1ad, широко известный под довольно понятным названием “QinQ” (протокол q внутри протокола q). Суть этого протокола состоит в добавлении второй метки VLAN для обеспечения возможности разбиения на VLAN-ы 2-го уровня, VLAN протокола 801.1q. Такая потребность возникает например, при разбиении на внутрикорпоративные VLAN-ы “внешней” VLAN, арендованной у некоторого оператора связи.

Положение в заголовке кадра и формат метки VLAN. Метка VLAN имеет длину 4 байта и размещается в заголовке кадра сразу после адресов получателя и отправителя. Рассмотрим 3 поля, входящих в эту метку: признак поля метки VLAN, тег протокола 802.1q (протокола передачи между коммутаторами меток VLAN), и тег протокола 802.1p (протокола приоритезации пакетов) и признак трансляции протокола канального уровня.

Признак поля метки VLAN имеет длину 2 байта и содержит фиксированное значение кода поля метки. Это поле занимает в структуре заголовка кадра то же место, что и поле длина/протокол. И указанный в этом поле код позволяет идентифицировать его как часть метки VLAN, а не как код протокола более высокого уровня или длину кадра.

Поле тега 802.1q располагается в 12 младших битах поля метки. Длина этого поля позволяет разместить в нем 4094 значения номеров VLAN (значения 0 и 4095 являются служебными).

Поле тега 801.1p располагается в 3-х старших битах 3-го байта метки и предназначено для размещения в нем приоритета кадра.

Отметим, что применение указанных протоколов возможно лишь при соответствующем увеличении максимального размера кадра MTU. При применении протокола 801.1q и/или 801.1p требуется обеспечение MTU=1522 (вместо стандартного для сетей Ethernet MTU=1518). При применении протокола 801.1ad требуемым значением MTU является 1526.

И оставшийся бит (4-й бит 3-го байта поля метки) используется как признак трансляции протокола канального уровня. Если значение этого бита установлено в “1”, то это значит, что передаваемый кадр является кадром FDDI или Token Ring, а не кадром Ethernet. Таким образом к традиционный прозрачный режим работы коммутаторов для некоторых кадров может быть заменен транслирующим режимом.

Транковые каналы. Транковыми (trunk - магистраль) называются каналы между коммутаторами, порты подключения к которым не помечены как принадлежащие какой-либо VLAN, а специальным образом сконфигурированные как транковые, предназначенные для пересылке через эти каналы помеченных кадров в протоколе 802.1q. Отметим, что при конфигурировании транковых каналов несколько однонаправленных (соединяющих одну и ту же пару коммутаторов) физических канала

могут объединяться в один логический транковый канал, пропускная способность которого равна сумме пропускных способностей объединенных каналов. Для каналов, несущих трафиковую нагрузку нескольких VLAN-ов, потребность в возможности повышения их пропускной способности зачастую актуальна.

3.1.4. Основные выводы по развитию технологий семейства Ethernet

В результате рассмотренного в настоящем параграфе развития изначально шинных технологий Ethernet, выполненного с середины 1990-х годов по время написания настоящих строк были полностью преодолены все недостатки, свойственные сетям с шинной технологией, и разработаны технологии создания сетей канального уровня (уровня 2), обладающих высокими показателями быстродействия, надежности и масштабируемости (как по количеству подключенных к сети компьютеров так и по протяженности кабельных систем). При этом по показателю быстродействия технология 100Gigabit Ethernet была абсолютным лидером с 2010 года и до момента появления в 2017 году мультиплексоров STM-1024 технологии SDH, обеспечивающих передачу данных со скоростью 160 Гбит/сек. Но, весьма вероятно, что уже скоро будут завершены работы по созданию стандартов 200Gigabit Ethernet и 400Gigabit Ethernet, и статус-кво технологий Ethernet по показателю быстродействия будет восстановлен.

Кроме отмеченных достоинств современные технологии Ethernet обеспечивают безопасное совместное использование общей физической инфраструктуры канального сетей уровня различными группами пользователей и/или распределенными сетевыми приложениями (например, системой видеонаблюдения), предоставляя возможность создания наложенных на эту инфраструктуру виртуальных сетей VLAN (называемых также L2VPN), абсолютно изолированных друг от друга на канальном уровне (напомним, что VLAN'ы не взламываются). Некоторым недостатком VLAN'ов (L2VPN) является их "беззащитность" при перегрузке другими VLAN'ами совместно используемых транковых каналов, приводящей к нежелательным потерям доступной канальной емкости. Поэтому транковые каналы должны обладать достаточно высоким резервом их свободной емкости.

При этом сети Ethernet могут применяться не только при создании транспортной инфраструктуры абонентских компьютерных сетей различного масштаба (от простых "домашних" сетей до корпоративных сетей крупных территориально распределенных организаций), магистральных сетей операторов связи различного масштаба (от местного до национального), сетей FTTB (Fiber to the Building - оптика до здания), но и для создания сетей управления сложными техническими объектами и технологическими процессами. Последняя возможность обеспечивается, в частности, рыночной доступностью конверторов Ethernet интерфейсов для разнообразных датчиков (температуры, давления, угла поворота и других аналогово-цифровых преобразователей) и исполнительных механизмов (переключателей, электродвигателей и пр.).

В силу отмеченных достоинств технологий семейства Ethernet и устойчивого темпа их развития автор полагает, что в будущем области возможного применения этих технологий будут только расширяться.

3.2. Технология WiFi

Технология WiFi, определяемая стандартом IEEE 802.11, как и другие 802-е технологии и протоколы IEEE, является технологией семейства Ethernet. Но, в отличие от других технологий этого семейства, она базируется на использовании радиосреды, а не кабельных систем для передачи данных, что вносит ряд рассматриваемых ниже особенностей и новшеств в применяемые методы передачи данных через общую шинную среду.

3.2.1. Стандарты IEEE 802.11

Семейство стандартов IEEE 802.11 выросло из беспроводной технологии подключения кассовых аппаратов, разработанной в 1991 году корпорацией NCR. Впоследствии один из разработчиков NCR - Вик Хейз был назначен руководителем комитета IEEE по созданию стандарта беспроводной сетевой связи. И в 1997 вышел в свет первый стандарт IEEE 802.11, работающий на скоростях 1 или 2 Мбит/с. Через 2 года были выпущены еще два стандарта: 802.11a и 802.11b. Первый работал на высокой по тем временам (но в то время занятой военными) частоте 5 ГГц и передавал данные на скорости до 54 Мбит/с. Второй - 802.11b использовал тот же диапазон частот 2.4 ГГц, что и исходный стандарт 1997 года, и обеспечивал скорость 11 Мбит/с. В то время изготовить устройства, функционирующие синхронно на высоких скоростях, было сложно. Передатчики/приемники сигнала различных производителей оказывались несовместимы между собой. Поэтому в 1999 году компании-пионеры беспроводных технологий сформировали WiFi-альянс, занимающийся тестированием беспроводного оборудования на соответствие стандартам. Устройства, успешно прошедшие тест, имели право распространяться под новой торговой маркой WiFi. Высокочастотные устройства стандарта 802.11a начали производится гораздо позже, чем стандарта b, когда последние уже заполонили рынок. Поэтому, когда в 2003 году вышел работающий на той же частоте 2.4 ГГц и совместимый с b стандарт 802.11g, передающий данные со скоростью 54 Мбит/с, производители и пользователи перешли с b сразу на g. Сейчас повсеместно распространен стандарт 802.11n 2009 года с пропускной способностью до 150 Мбит/с (600 Мбит/с при использовании технологии MIMO и 4х антенн). Но есть и более высокоскоростные стандарты: ac, ad, а также стандарты для особых областей применения.

Работа большинства WiFi оборудования в зависимости от условий ограничена расстоянием в несколько десятков метров. Однако существуют устройства, которые позволяют передавать WiFi сигнал на несколько десятков километров. В основном это делается за счет использования направленных антенн.

В пределах допустимого диапазона частот 2.4 – 2.485 ГГц или 5.15 – 5.725 ГГц WiFi-устройства используют один из набора перекрывающихся каналов шириной 20 или 40 МГц соответственно. Для первого диапазона 2.4 – 2.485 ГГц существует всего 13 каналов по 20 МГц, из них максимум 4 можно выбрать полностью не перекрывающимися. Это приводит к проблемам в многоквартирных домах с высокой плотностью точек доступа WiFi. Устройства, использующие общий или соседние каналы мешают друг другу. Проблему решают установкой другого номера канала в настройках точки доступа или переходом на более свободный и широкий диапазон частот: 5.15 – 5.725 ГГц, в котором больше сотни каналов.

3.2.2. Архитектура

Одна из возможных схем WiFi-сети представлена рис. 3. Она состоит из двух стандартных зон BSS (Basic Service Set), управляемых точкой доступа и WiFi-маршрутизатором и идентифицируемые идентификатором SSID. WiFi-зоны типа BSS являются независимыми, и без дополнительного конфигурирования перемещение пользователя из одной зоны в другую не поддерживается (даже если сети будут иметь одинаковые идентификаторы SSID (Service Set Identifier) и частотные каналы). Для организации покрытия большой площади и функции мобильности клиентов стандартные WiFi зоны объединяют в одну зону расширенного типа ESS (Extended Service Set, см. рис. 4). Такая WiFi-сеть с точки зрения канального уровня функционирует как повторитель (мост), реализуя общую среду передачи данных, хотя на самом деле каждое устройство подключено к своей точке доступа. Все входящие в одну ESS-зону WiFi-сети должны иметь одинаковый идентификатор SSID и настройки шифрования.

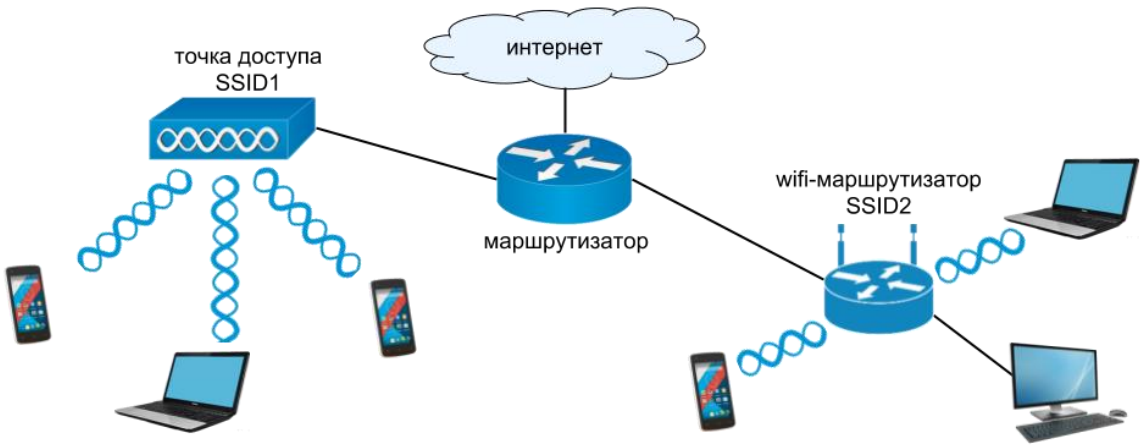

Рис. 3. Схема сети с двумя стандартными зонами WiFi

Рис. 4. Схема WiFi-зоны расширенного типа с двумя основными и одной удаленной базовыми станциями

Точки доступа каждые 0,1 сек с помощью сигнальных пакетов-маяков рассылают идентификатор WiFi-сети (SSID). Клиенты сканируют все частотные каналы в поисках сигнальных пакетов. Получив полный список находящихся в окрестностях WiFi-сетей, клиент принимает решение о подключении к одной из них и отправляет запрос на аутентификацию. В крупных WiFi-сетях точка доступа обычно перенаправляет этот запрос к специализированному серверу аутентификации, используя такой протокол как RADIUS. Перенос функции аутентификации с точек доступа на отдельный сервер позволяет легко администрировать набор допустимых пользователей вне зависимости от размера WiFi сети.

Существует еще третий тип WiFi-зон: IBSS (Independent Basic Service Set). Такие WiFi сети функционируют без точки доступа, узлы передают пакеты напрямую друг другу, поэтому зачастую такой режим называют ad-hoc (произвольный) или P2P, в противоположность режиму с инфраструктурой (infrastructure).

2.3.3. Протокол доступа к среде передачи

Разработчики стандарта 802.11 приняли решение использовать в WiFi тот же протокол доступа к общей среде передачи данных, что и в завоевавшей большую популярность технологии Ethernet. Для адаптации к беспроводным сетям протокол CSMA/CD пришлось немного изменить. Детектирование коллизий пакетов, легко

проводимое в проводных сетях, очень сложно реализовать в радиосвязи: одновременный прием и отправка сигнала приведут к поломке приемника, так как он рассчитан на приходящие от других станций сигналы с амплитудой на несколько порядков меньше излучаемой. Таким образом в WiFi отправитель, начав передавать пакет, не останавливается вплоть до конца передачи. В сетях с большим числом коллизий такое поведение может привести к существенному уменьшению пропускной способности, поэтому применяется ряд приемов, предотвращающих коллизии. Отсюда происходит и название протокола доступа: CSMA/CA (Collision Avoidance) в отличие от CSMA/CD (Collision Detection) в Ethernet.

Предотвращение коллизий происходит по следующему протоколу. Перед передачей узел проверяет свободен ли канал. Если да, то происходит передача. В противном случае, узел ждет освобождения канала. Но но при этом узел начинает передачу не сразу после освобождения, а через случайный интервал времени, если канал не оказался опять занят. Временной интервал должен быть случайным, чтобы не допустить одновременной отправки пакетов нескольким станциями, которые вместе ждут освобождения канала. Вероятность совпадения случайных временных промежутков достаточно мала. Получатель после приема сообщения проверяет его контрольную сумму CRC и, в случае отсутствия искаженных битов, отвечает коротким пакетом-подтверждением успешности передачи. Отправитель пакета, в случае отсутствия подтверждения в течении определенного времени, опять выжидает случайное время и еще раз пытается передать пакет. После нескольких неудачных попыток пакет отбрасывается.

Рассмотрим формат кадра WiFi (см. рис. 5)

2	2	6	6	6	2	6	0-2312	4
управ-ление	длите-льность	адрес1	адрес2	адрес3	№ кадра	адрес4	данные	CRC

Рис. 5. Формат кадра 802.11. Вверху указаны размеры полей в байтах

Кадр WiFi состоит из 9 полей :

1. Поле управления (2 байта), содержащее версию протокола, тип и подтип кадра, направление передачи (к/от точки доступа), признак использования шифрования и т.д.
2. Протокол 802.11 позволяет устройствам резервировать канал на время, указанное в поле “Длительность”

3-5. Три MAC-адреса: 1 - адрес WiFi-получателя кадра, 2 - адрес WiFi-отправителя, 3 - MAC адрес порта маршрутизатора, к которому подключена точка доступа

6. Номера кадра используется в подтверждениях об успешной доставке данных
7. Четвертый адрес нужен в ad-hoc WiFi сетях
8. В поле данных разрешено пересылать до 2312 байт, но на практике обычно его размер совпадает с рекомендованным для Ethernet.
9. Поле контроля ошибок CRC

В инфраструктурных WiFi сетях (с точкой доступа) все пересылаемые пакеты проходят через точку доступа, поэтому один из MAC-адресов: адрес1 или адрес2 всегда принадлежит точке доступа. При отправке пакета от одного клиента WiFi сети к другому (а не маршрутизатору) поле адрес3 заполняется MAC-адресом клиента-получателя.

3.2.4. Безопасность

Беспроводные сети по сравнению с кабельными очень уязвимы с точки зрения безопасности. Первый стандарт шифрования трафика появился вместе с 802.11 и имел дерзкое название WEP — Wired Equivalent Privacy (безопасность, эквивалентная проводной). Но из-за особенностей динамической смены ключей при отправке большого числа пакетов этот стандарт позволял после выполнения некоторого анализа подобрать ключи шифрования, что было открыто в 2001 году Скоттом Флурером, Ицик Мантином и Ади Шамиром. Впоследствии было предложено еще несколько более эффективных схем взлома WEP, которые полностью дискредитировали этот стандарт.

Ключевая проблема WEP заключается в использовании слишком похожих ключей для различных пакетов данных. Пришедшие на смену стандарты шифрования WPA и WPA2 (Wi-Fi Protected Access) применяют технологию построения иерархии динамических ключей TKIP (Temporal Key Integrity Protocol), которые по определенному алгоритму выбираются для шифрования каждого отдельного пакета данных. WPA также использует механизм проверки целостности сообщений MIC (Message Integrity Check), чтобы можно было сразу различить измененные пакеты или отправленные в сеть злоумышленником. Вторая версия стандарта WPA2 использует выбранный на конкурсной основе новый криптографический алгоритм AES (Advanced Encryption Standard).

Наряду с шифрованием для защиты WiFi-сетей также используется фильтрация MAC-адресов, а также сокрытие идентификатора сети SSID.

3.2.5. MIMO

При сложении волн одинаковой частоты от разных источников можно наблюдать возникновение стационарных пространственных структур (см. рис. 6). В некоторых направлениях колебания в волне удваиваются, а в некоторых – сходят на нет. В помещении с одним источником радиоволн такие структуры образуются за счет сложения прямого сигнала и отраженных от стен, потолка. Этот эффект называется многолучевым распространением. При попадании приемника в точку минимума колебаний будут наблюдаться проблемы со связью. Ситуация осложняется еще и тем, что возникающие структуры максимумов и минимумов колебаний меняются со временем.

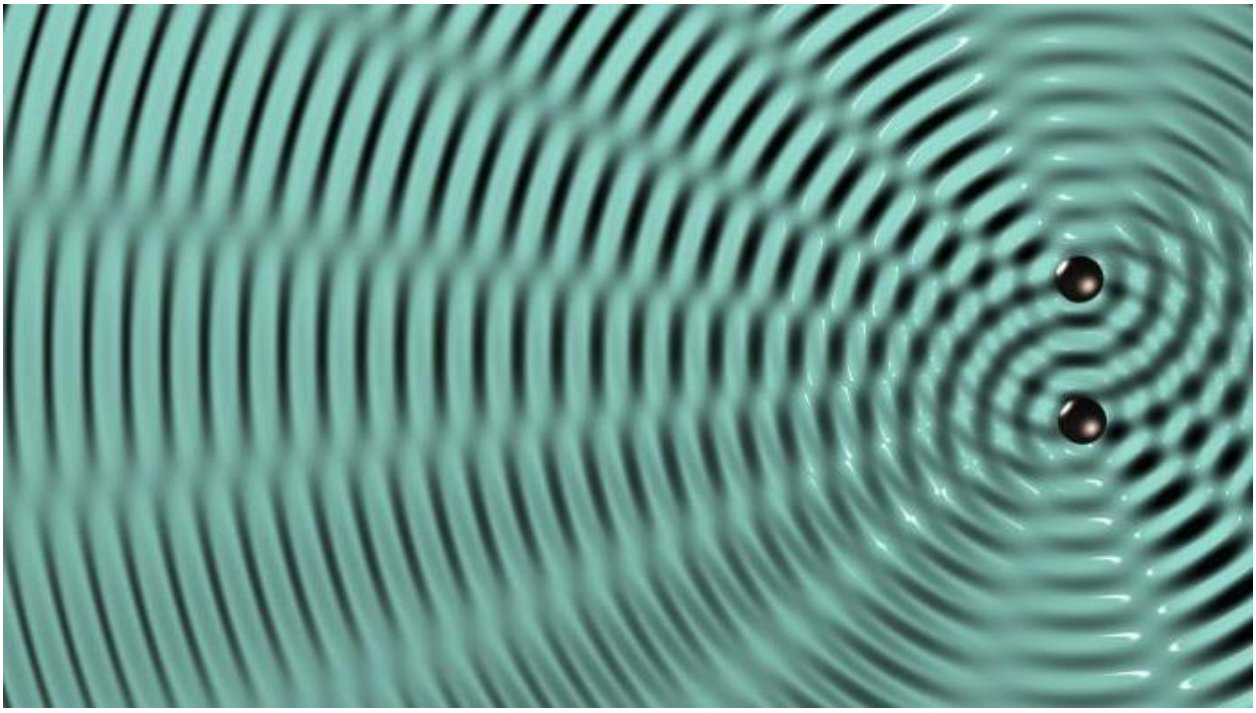

Рис.2.16. Интерференция волн от двух когерентных источников

Увеличение качества и скорости передачи по радиоканалу можно осуществить за счет использования метода пространственного кодирования сигнала MIMO, в котором передача и/или прием данных осуществляются несколькими антеннами (MIMO — Multiple Input Multiple Output). Первые попытки использования нескольких антенн предпринимались уже давно. Использование нескольких приемных антенн позволяет сложить (с некоторыми весовыми коэффициентами, зависящими от условий) приходящие сигналы и таким образом существенно повысить соотношение сигнал/шум в приемнике. В 1997 году Аламоути предложил альтернативную схему повышения качества сигнала в точке приема, использующую несколько передатчиков и один приемник — *пространственно-временное кодирование*. Передатчики отправляют избыточные копии данных в надежде, что хотя бы одна из них достигнет получателя в целости. Данная

схема подходит для зашумленных каналов с маленьким значением отношения сигнал/шум в точке приема.

В случае хорошего качества связи увеличить скорость передачи при наличии нескольких антенн у приемника и у передатчика можно за счет *пространственного мультиплексирования*. В этом типе связи разные антенны передатчика отправляют разные части потока данных. Искажаясь сигнал достигает приемных антенн, и далее начинает работать математический алгоритм, определяющий, какие данные привели к такому приемному сигналу. В простейшем случае — это полный перебор всех комбинаций битов. Для корректного декодирования приемник должен знать так называемую передаточную функцию, описывающую искажение сигнала по пути от отправителя к получателю. Для ее вычисления в схеме MIMO резервируется часть частот спектра.

Кроме WiFi технология MIMO также используется в WiMAX и в системах мобильной связи.

3.2. Мобильный доступ в интернет

В 80-х годах прошлого века в разных странах строились свои сети мобильной связи, основанные на фирменных стандартах, в основном с аналоговой модуляцией голоса. Европейские страны, зная, что им не победить поодиночке в технологической борьбе со странами, обладающими гораздо более крупным рынком, решили объединиться в создании общего свободного стандарта цифровой мобильной связи. Работы начались в 1982 после создания комитета GSM (Groupe Special Mobile), который занялся разработкой спецификаций собственного стандарта мобильной связи. Пять лет спустя были подписаны первые официальные международные соглашения, в 1991 году начала функционировать первая коммерческая сеть GSM, а к 1993 году GSM сети функционировали уже в десятках стран, и акроним GSM приобрел новый смысл - Global System for Mobile communications. Так началась новая эра беспроводной телефонии 2G (**G**eneration - поколение), а предыдущая получила название 1G.

Сети GSM работают на частоте около 900 МГц и 1800 МГц. Для сеанса связи каждому мобильному устройству выделяется пара частот: для входящего и исходящего сигналов. Вместе с частотным разделением (FDMA) в GSM также используется и временное (TDMA). Время делится на кадры размером 4.6 мс, по 8 тайм-слотов каждый. Таким образом, одну частоту могут использовать несколько пользователей (с применением разных временных слотов).

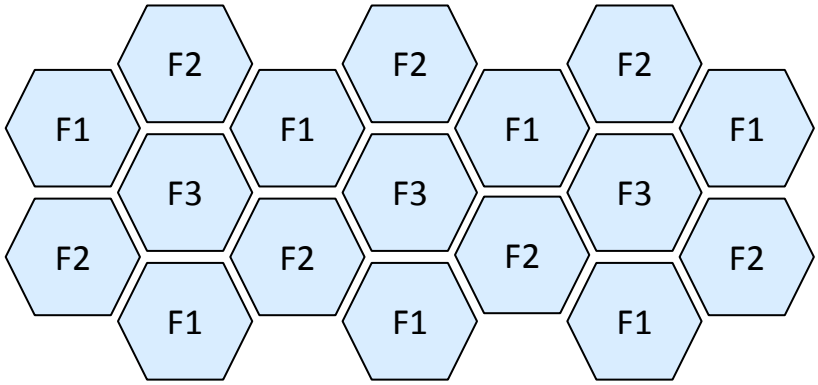

Рис. 7. Зона покрытия сети. F1,F2,F3 - частоты ячеек

Зона покрытия сети делится на ячейки - соты, отсюда и возникло название “сотовая связь”. Смежные соты используют разные частотные диапазоны, благодаря чему наложение сигналов антенн на границе не вызывает проблем со связью (см. рис. 7). Сотовые ячейки могут иметь различный размер от 300 метров до 35 километров. Большие соты со временем, если количество пользователей сильно увеличилось, дробят на несколько сот (обычно 3) меньшего диаметра.

Благодаря цифровой технологии передачи сигналов GSM сеть может использоваться и для передачи данных. Первый стандарт CSD (Circuit Switched Data), позволял передавать данные со скоростью 9.6 Кбит/с и использовал один голосовой тайм-слот. Во время всего сеанса связи, даже несмотря на возможные перерывы в передачи данных, выделенный таймслот не мог использоваться другими абонентами. Таким образом, технология CSD реализовала коммутацию каналов, что непосредственно следует из ее названия. Следующий стандарт передачи данных GPRS реализовал коммутацию пакетов и использовал общую среду передачи более эффективно. В GPRS несколько абонентов могут использовать одни и те же таймслоты. Каждый кадр временной шкалы делится на две части: маленький промежуток резервации и набор временных слотов данных. Во время резервации абоненты, используя протокол Slotted ALOHA, резервируют один или несколько слотов для передачи данных. При этом возможны коллизии. Далее наступает интервал передачи данных, в котором коллизии невозможны. Такой протокол доступа к общей среде передачи данных называется Reservation ALOHA.

В начале 2000-х мобильное ПО было довольно слабо развито. Из-за этого крупнейшие провайдеры сотовой связи создали упрощенную технологию доступа к всемирной паутине - WAP (Wireless Application Protocol). Стандарт содержал описание адаптированного протокола HTTP, набора сопутствующих протоколов, языка разметки аналогичного HTML для качественного отображения контента веб-страниц на монохромных (а позже и четырёх- и восьмицветовых) экранах мобильных устройств. Но с появлением смартфонов необходимость в WAP исчезла.

Переход к коммутации другого типа в GPRS потребовал усложнения схемы GSM сети. Теперь общую среду передачи должны были разделять голосовые соединения с их собственной маршрутизацией звонков и пакеты передачи данных с маршрутизацией по протоколу IP. При этом те и другие устройства маршрутизации использовали общие базы данных абонентов, устройств и т.д. Впоследствии данная схема инфраструктуры, названная *базовой сетью GPRS* (GPRS core network), была перенесена на стандарт связи третьего поколения 3G (см. рис. 8). Ключевые элементы схем базовых сетей GPRS второго и третьего поколений имеют разные названия (чтобы не было путаницы на совместных графиках), но очень похожие функции.

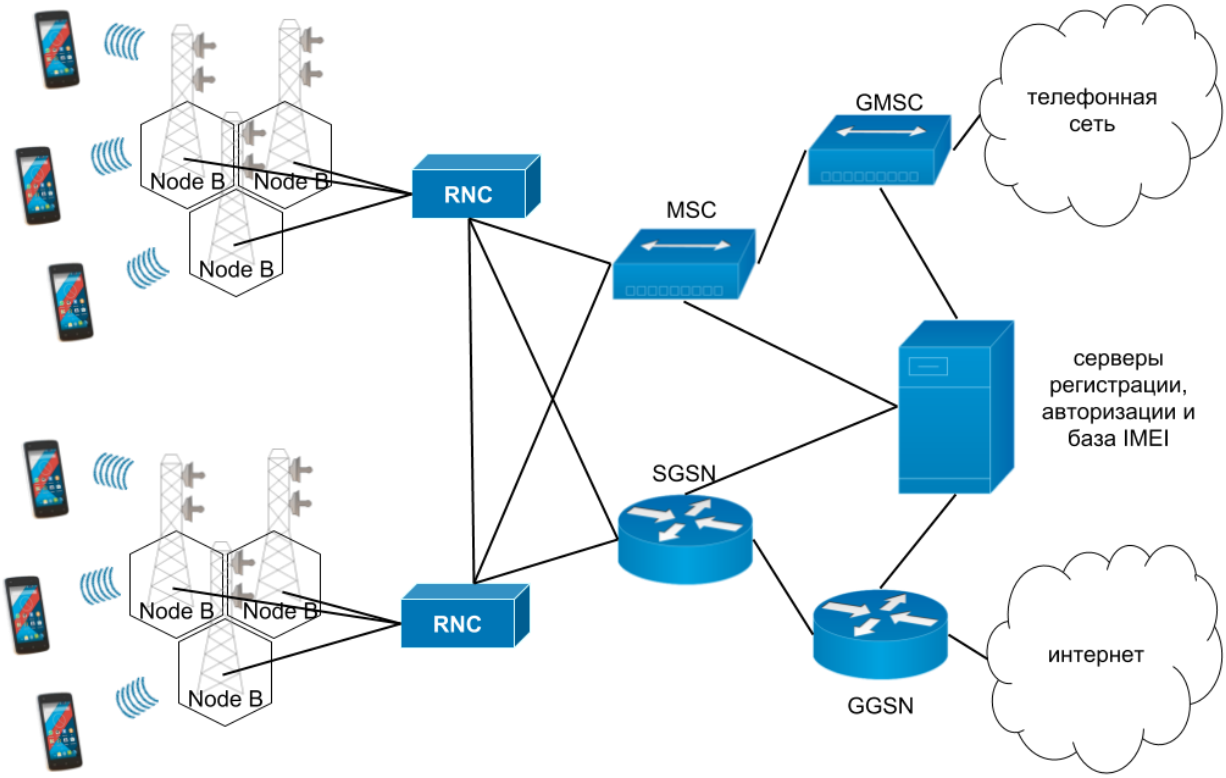

Рис. 8. Схема сети 3G

Так как сети 2G в некоторых странах уже выведены из обращения, рассмотрим схему базовой мобильной сети передачи данных третьего поколения UMTS (Universal Mobile Telecommunications System, см. рис. 8). Так же как и сети 2G она была спроектирована как пристройка к существующей сети голосовых данных. Заменить функции голосовой сети и организовать единую инфраструктуру на основе протокола IP решились только разработчики стандарта четвертого поколения LTE. Голосовые сигналы и зашифрованные данные от мобильных телефонов через базовые станции Node B поступают в контроллер радиосети RNC (Radio Network Controller). Главной функцией RNC является управление доступом к общей среде передачи данных. В UMTS используется другой тип разделения канала: так же, как в сетях 2G, временная шкала делится на слоты, но внутри одного таймслота устройства применяют кодовое разделение CDMA, которое обеспечивает гораздо бóльшую емкость сети. Контроллеры RNC осуществляют распределение таймслотов и кодов в CDMA, участвуют в операции хэндовер — переподключения перемещающегося абонента от одной базовой станции к другой, шифрование и расшифровку данных. Поступившие от базовой станции данные, в зависимости от типа, RNC передает голосовому коммутатору MSC (Mobile Switching Center) или узлу SGSN (Serving GPRS Support Node) обслуживания абонентов GPRS, контролирующему доставку пакетов, занимающемуся преобразованием форматов пакетов GSM↔TCP/IP, регистрацией (прикреплением) подключившихся абонентов, шифрованием и подсчетом статистики. Через специальные шлюзы GMSC и GGSN абоненты подключаются к телефонной сети общего назначения и сети интернет.

По поводу стандарта четвертого поколения долго шли напряженные дебаты по поводу выбора между WiMAX от IEEE и LTE от 3GPP. Разработанный на несколько лет раньше WiMAX (IEEE 802.16) изначально был предназначен для беспроводного высокоскоростного подключения фиксированных абонентов. Институт математики, механики и компьютерных наук Южного федерального университета гордится тем, что одним из руководителей технической группы WiMAX Forum был выпускник и бывший преподаватель матанализа Владимир Григорьевич Яновер, ученик профессора И.Б. Симоненко. Вышедшая в 2005 году мобильная версия стандарта WiMAX была взята некоторыми провайдерами за основу построения беспроводных сетей нового типа. Таким образом, инициативу разработки новых стандартов мобильной связи попытался перехватить комитет IEEE. Но европейский консорциум 3GPP не отставал. Его специалисты, взяв за основу ту же модуляцию сигнала, что и в WiMAX, придумали стандарт LTE, который можно было внедрять параллельно с существующими сетями 2G и 3G, используя часть их инфраструктуры. Такой подход экономически оказался гораздо выгоднее для мобильных провайдеров, чем построение сети “с нуля”. Поэтому в мобильных сетях стандарт LTE стал победителем. Несмотря на это, многие беспроводные сети интернет-провайдеров в России и других странах используют технологию WiMAX.