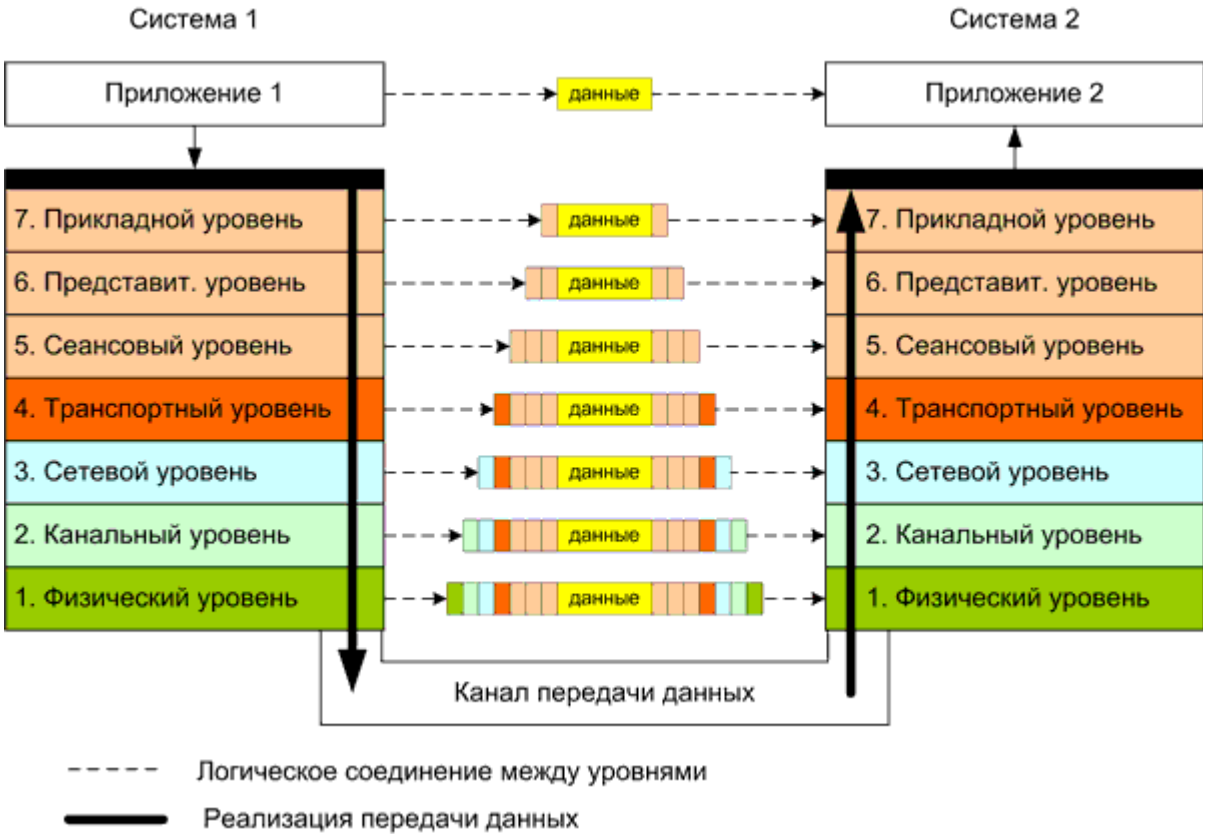
42. Протоколы канального уровня. Сети WiFi. Стандарты. *Физическое и логическое кодирование данных (Береснев зачеркнул)*. **Алгоритмы разделения канала.**

Модель OSI



Канальный уровень (data link layer)
Основные функции:

- Обеспечивает формирование фреймов (frames) — кадров;
- Обеспечивает контроль ошибок и управление потоком данных (data flow control);
- Логическое кодирование данных.

Примеры протоколов:
ATM, Ethernet, EAPS (Ethernet Automatic Protection Switching), FDDI (Fiber Distributed Data Interface), MPLS (Multiprotocol Label Switching), PPP (Point-to-Point Protocol), SLIP (Serial Line Internet Protocol)

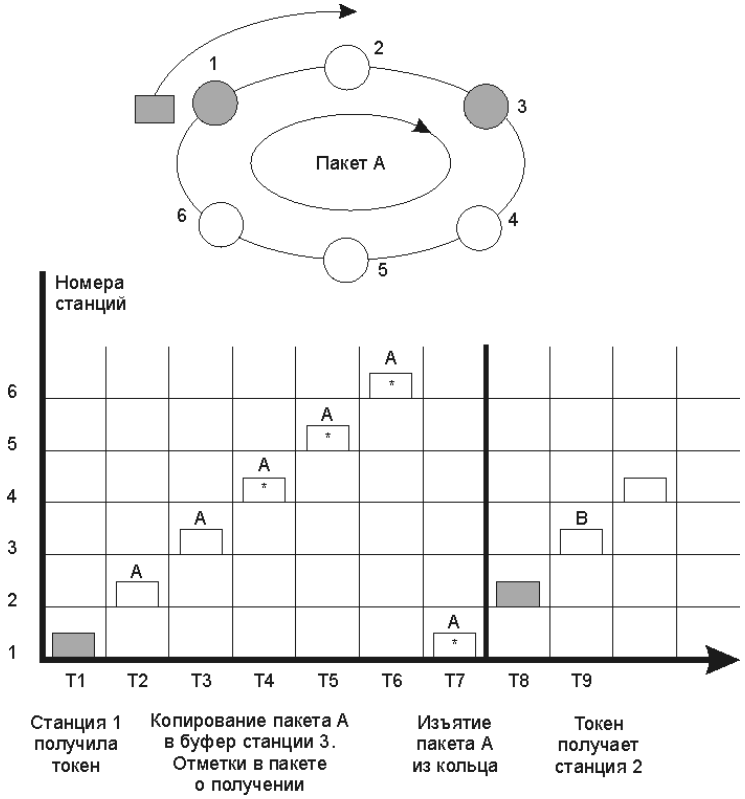
Token Ring:
Технология была разработана компанией IBM в 1984 году.
В 1985 году комитет IEEE 802 на её основе разработал стандарт 802.5.
По сравнению с аппаратурой Ethernet аппаратура Token-Ring оказывается заметно дороже, так как использует более сложные методы управления обменом, поэтому распространена сеть Token-Ring значительно меньше. Однако ее применение становится оправданным, когда требуются большие интенсивности обмена (например, при связи с большими компьютерами) и ограниченное время доступа.

	Token Ring	IEEE 802.5
Скорость передачи данных	4,16 Мбит/с	4,16 Мбит/с
Кол-во станций в сигменте	260 (экранированная витая пара) 72 (неэкранированная витая пара)	250
Топология	Звезда	Не специализировано
Кабель	Витая пара	Не специализировано

Характеристики:

- Сети Token Ring используют разделяемую среду передачи данных – кольцо;
- Для доступа к среде используется алгоритм основанный на передаче станциями права на использование кольца в определенном порядке (детерминированная сеть);
- Право на использование кольца передается с помощью кадра специального формата, называемого маркером или токеном;
- Две скорости работы: 4 и 16 Мбит/с;
- Определены процедуры контроля работы сети (активный монитор)
- Выбирается во время инициализации кольца по максимальному MAC-адресу;

Доступ с передачей токена



Физический уровень Token Ring:

MAU/MSAU (Multi-station Access Unit) – устройство многостанционного доступа:
- пассивные (простое соединение в кольцо);
- активные (усиление, регенерация, синхронизация сигналов).

TCU (Trunk Coupling Unit) – устройство подключение к магистрали

FDDI

FDDI (Fiber Distributed Data Interface) – распределённый интерфейс передачи по оптоволокну.

Данная технология во многом основывается на Token Ring, развивая и совершенствования её идеи.

Институт ANSI разработал с 1986 по 1988 гг. начальную версию стандарта для скорости 100 Мбит/с по двойному кольцу длиной 100 км.

Параметры:

- В технологии FDDI используется метод логического кодирования 4B/5B;
- Метод физического кодирования – NRZI;
- Тактовая частота передачи 125 МГц.
- В нормальном режиме данные передаются только по одному кольцу из пары – первичному (primary). Вторичное (secondary) кольцо используется в случае отказа части первичного кольца.
- По первичному и вторичному кольцам данные передаются в противоположных направлениях, что позволяет соблюсти порядок узлов сети при подключении вторичного кольца к первичному.
- В случае нескольких отказов, сеть FDDI распадается на несколько отдельные (но функционирующих) сетей.

Виды трафика

Технология FDDI предусматривает передачу двух типов трафика в сети:

- Синхронный трафик
- Асинхронный трафик

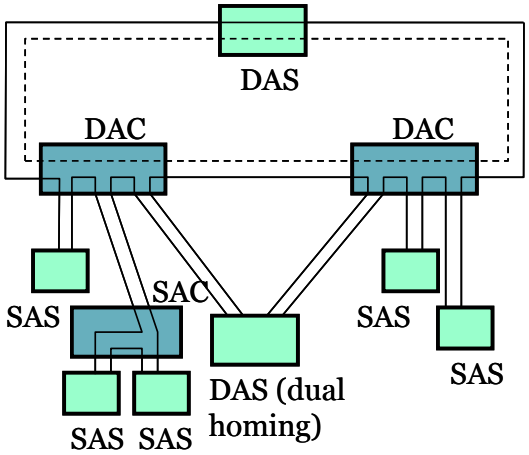
Синхронный трафик образуют приложения, для которых критичным является наличие временной задержки при передаче данных – передача голоса или видео информации. Остальные данные, которые передаются по сети, образуют асинхронный трафик. Синхронный передается всегда, независимо от загруженности кольца. Асинхронный может произвольно задерживаться.

Каждой станции выделяется часть полосы пропускания, в пределах которой станция может передавать синхронный трафик. Часть полосы пропускания кольца, которое остается, отводится под асинхронный трафик.

Маркерный метод доступа:

- FDDI использует маркерный метод доступа, близкий к методу доступа сетей Token Ring. Основное отличие – в плавающем значении времени удерживания маркера для асинхронного трафика: при небольшой загрузке сети время содержания растет, а при перегрузках – уменьшается.
- Во время инициализации кольца узлы договариваются о максимально допустимом времени оборота маркера по кольцу T_Opr. Для синхронного трафика время содержания маркера не изменяется. Для передачи синхронного кадра узел всегда имеет право захватить маркер и удерживать его в течении заданного фиксированного времени.
- Если узел хочет передать асинхронный кадр, он должен измерять время оборота маркера (Token Rotation Time, TRT) – интервал между двумя прохождениями маркера через него. Если кольцо не перегружено (TRT<T_Opr), то узел может захватить маркер и передать свой кадр (или кадры) в кольцо, при этом допустимое время содержания маркера THT=T_Opr-TRT. Если кольцо перегружено (TRT>T_Opr), то узел не имеет право захватывать маркер.

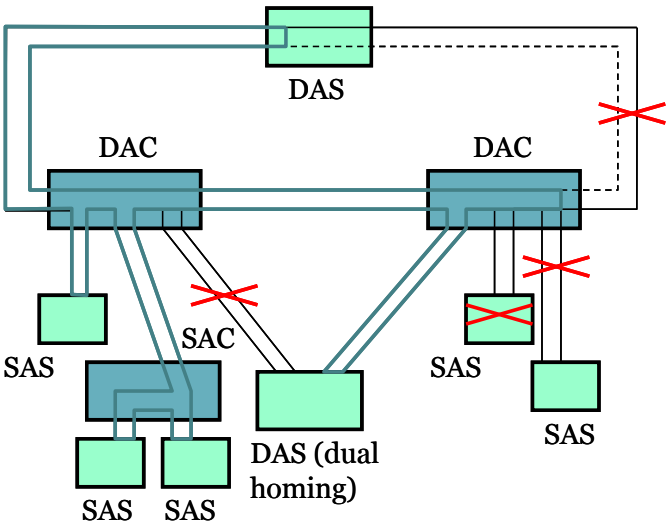
Подключение станций в FDDI



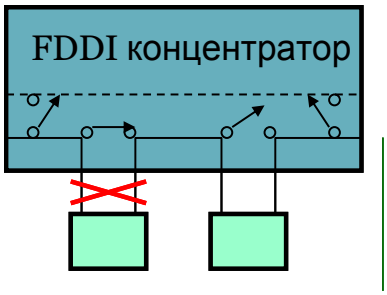
SAS (Single Attachment Station) - подсоединение станции только к одному из колец
DAS (Dual Attachment Station) - подсоединение станции к двум кольцам, повышается отказоустойчивость
SAC, DAC (Single, Dual Attachment Concentrators)

Dual Homing - двойное подключение станции к одному из колец (также повышает надежность соединений, один из портов - запасной)

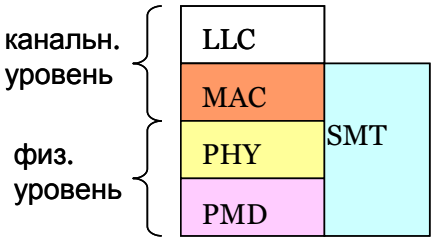
Сворачивание колец



На каждом порте концентратора и в сетевой карте есть так называемый обходной переключатель (bypass switch). Его назначение - отключать аппаратуру, подключенную к порту от кольца в случае нештатных ситуаций.



Структура стека FDDI



Media Access Control (MAC) (Управление доступом к носителю) - способ доступа к носителю, формат кадра, обработка маркера, адресация, алгоритм CRC (проверка контрольной суммы) и механизмы устранения ошибок.
Physical Layer Device (PHY) (Устройство физического уровня) - кодирование 4B/5B, требования к синхронизации (управление эластичным буфером для согласования частоты входных и выходных сигналов), формированию кадров и другие функции.
Physical Media Dependent (PMD) - требования к мощности, длине волны оптических сигналов, к многомодовому оптоволоконному кабелю 62.5/125 мкм, к оптическим обходным переключателям (optical bypass switches) и оптическим приемопередатчикам, параметры оптических разъемов MIC (Media Interface Connector), их маркировка.

SMT(station mamagement)
SMT (управление станциями) - конфигурация станций FDDI, конфигурация кольцевой сети и особенности управления кольцевой сетью, включая вставку и исключение станций, инициализация, изоляция и устранение неисправностей, составление графика и набор статистики.
Все узлы обмениваются SMT кадрами (нет активного монитора).
SMT управляет другими уровнями: с помощью уровня PHY устраняются отказы сети по физическим причинам, например, из-за обрыва кабеля, а с помощью уровня MAC - логические отказы сети, например, потеря кадров данных между портами концентратора.

Инициализация кольца:
В ходе процесса Claim Token всем станциям необходимо убедиться в работоспособности кольца и рассчитать максимальное время оборота токена. Наблюдается при:
- включении/выключении станции;
- утере токена;
- длительном отсутствии пакетов сквозь какую-нибудь станцию;
- по команде SMT.

Для этой процедуры каждая станция знает свое требуемое время оборота по кольцу. Оно должно быть в диапазоне 4-165мс и может назначаться администратором сети. Формируется кадр ZZZZ=0011 и в данных - требуемое время.
Станция, получившая Claim Token, генерирует пакет останова сети и запускает таймер. Если время превысит 165мс до завершения процедуры - начинается поиск неисправности в кольце. Если станция получает кадр с меньшим временем, то она перестает генерировать свой запрос.
При равных значениях преимущество имеют станции с большим MAC адресом. Первый оборот токена - служебный.

Преимущества
- высокая степень отказоустойчивости;
- способность покрывать значительные территории, вплоть до территорий крупных городов;
- высокая скорость обмена данными;
- возможность поддержки синхронного мультимедийного трафика;
- гибкий механизм распределения пропускной способности кольца между станциями;
- возможность работы при коэффициенте загрузки кольца близком к единице;
- возможность легкой трансляции трафика FDDI в трафики таких популярных протоколов как Ethernet и Token Ring за счет совместимости форматов адресов станций и использования общего подуровня LLC.

Сравнение технологий

Характеристика	**FDDI**	**Ethernet**	**Token Ring**
Битовая скорость	100 Мбит/с	10 Мбит/с	16 Мбит/с
Топология	Двойное кольцо деревьев	Шина/звезда	Кольцо/звезда
Метод доступа	Маркер (доля от времени оборота)	CSMA/CD	Маркер (система резерв. приоритетов)
Среда передачи	оптоволокно, STP	коакс., TP, оптоволокно	TP, оптоволокно
Макс. длина сети (без мостов)	200км (100км на кольцо)	2500м	1000м
Макс. расст-е между узлами	2км	2500м	100м
Макс. кол-во узлов	1000 соединений	1024	260
Тактирование и восстановление после отказов	Распределенная реализация тактирования и восстановления после отказов	Не определены	Активный монитор

Wi-Fi (англ. Wireless Fidelity — «беспроводная точность») — торговая марка Wi-Fi Alliance для беспроводных сетей на базе стандарта IEEE 802.11. Любое оборудование, соответствующее стандарту IEEE 802.11, может быть протестировано в Wi-Fi Alliance и получить соответствующий сертификат и право нанесения логотипа Wi-Fi.
Wi-Fi был создан в 1991 году NCR Corporation/AT&T (впоследствии — Lucent Technologies и Agere Systems) в Ньивегейн, Нидерланды. Изначально был разработан для систем кассового обслуживания. Под маркой WaveLAN был выеден на рынок и обеспечивал скорость передачи данных от 1 до 2 Мбит/с.
Создатель Wi-Fi (Wireless Fidelity) — Вик Хейз (*Vic Hayes*) находился в команде, по разработке таких стандартов, как:
- IEEE 802.11b;
- IEEE 802.11a;
- IEEE 802.11g.

В 2003 году Вик ушёл из Agere Systems. В 2004 году Agere Systems решила уйти с рынка Wi-Fi. Стандарт IEEE 802.11n был утверждён 11 сентября 2009 года.

Список стандартов
IEEE 802.11 — набор стандартов связи, для коммуникации в беспроводной локальной сетевой зоне частотных диапазонов 2.4, 3.6 и 5 ГГц.
При описании стандарта, в скобках указан год его принятия.
802.11 — Изначальный 1 Мбит/с и 2 Мбит/с, 2,4 ГГц и ИК стандарт (1997)
802.11a — 54 Мбит/с, 5 ГГц стандарт (1999, выход продуктов в 2001)

802.11b — Улучшения к 802.11 для поддержки 5,5 и 11 Мбит/с (1999)
802.11c — Процедуры операций с мостами; включен в стандарт IEEE 802.1D (2001)
802.11d — Интернациональные роуминговые расширения (2001)
802.11e — Улучшения: QoS, включение packet bursting (2005)
802.11F — Inter-Access Point Protocol (2003)
802.11g — 54 Мбит/с, 2,4 ГГц стандарт (обратная совместимость с b) (2003)
802.11h — Распределенный по спектру 802.11a (5 GHz) для совместимости в Европе (2004)
802.11i — Улучшенная безопасность (2004)
802.11j — Расширения для Японии (2004)
802.11k — Улучшения измерения радио ресурсов
802.11l — Зарезервирован
802.11m — Поддержание эталона; обрезки
802.11n — Увеличение скорости передачи данных (600 Мбит/с). 2,4-2,5 или 5 ГГц. Обратная совместимость с 802.11a/b/g . Особенно распространён на рынке в США в устройствах D-Link, Cisco и Apple. (сентябрь 2009)
802.11o — Зарезервирован
802.11p — WAVE — Wireless Access for the Vehicular Environment (Беспроводной Доступ для Транспортной Среды, такой как машины скорой помощи или пассажирский транспорт)
802.11q — Зарезервирован, иногда его путают с 802.1Q
802.11r — Быстрый роуминг
802.11s — ESS Mesh Networking (Extended Service Set - Расширенный Набор Служб; Mesh Network - Ячеистая Сеть)
802.11T — Wireless Performance Prediction (WPP, Предсказание Производительности Беспроводного Оборудования) — методы тестов и измерений
802.11u — Взаимодействие с не-802 сетями (например, сотовые сети)
802.11v — Управление беспроводными сетями
802.11x — Зарезервирован и не будет использоваться. Не нужно путать со стандартом контроля доступа IEEE 802.1X
802.11y — Дополнительный стандарт связи, работающий на частотах 3,65-3,70 ГГц. Обеспечивает скорость до 54 Мбит/с на расстоянии до 5000 м на открытом пространстве.
802.11w — Protected Management Frames (Защищенные Управляющие Фреймы)
Примечания:
802.11F и 802.11T являются рекомендациями, а не стандартами, поэтому используются заглавные буквы. Названия стандартов укорочены.

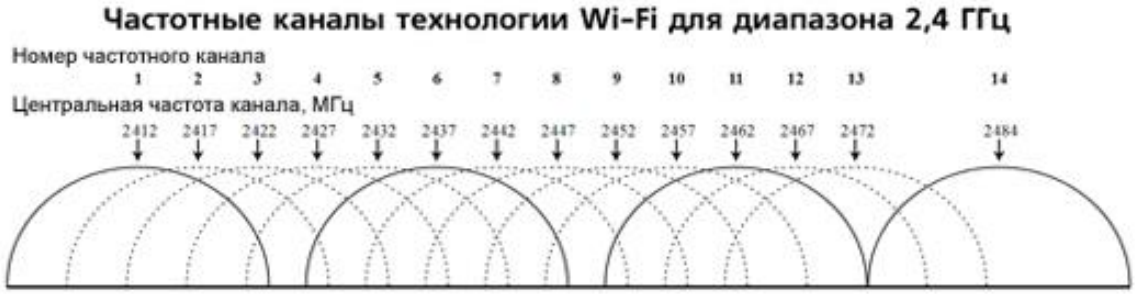
Сравнение стандартов

Технология	Стандарт	Скорость	Радиус действия	Частота
Wi-Fi	802.11a	До 54 Мбит/с	До 120 м	5 ГГц
Wi-Fi	802.11b	До 11 Мбит/с	До 140 км	2,4 ГГц
Wi-Fi	802.11g	До 54 Мбит/с	До 140 м	5 ГГц
Wi-Fi	802.11n	До 480 Мбит/с	До 250 м	2,4 или 5 ГГц
Wi-Max	802.16d	До 75 Мбит/с	6 – 10 км	1,5 – 11 ГГц
Wi-Max	802.16e	До 30 Мбит/с	1 – 5 км	2 - 6 ГГц

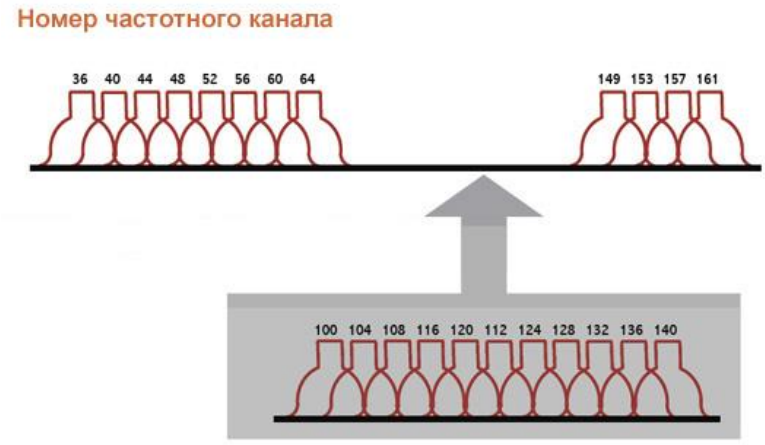
Стандарт IEEE	Название технологии на английском языке	Название технологии на русском языке	Частотный диапазон работы сетей,ГГц	Год ратификации WiFi альянсом	Теоретическая пропускная способность, Мбит/с	Реальная скорость передачи данных, Мбит/с
802.11 b	Wireless b	Стандарт «Би»	2,4	1999	11	5
802.11 a	Wireless a	Стандарт «Эй»	5	2001	54	20
802.11 g	Wireless g	Стандарт «Джи»	2,4	2003	54	20
	Super G	Технология «Супер Джи»	2,4	2005	108	40
802.11 n	Wireless N, 150Mbps	Технология «Эн 150»	2,4	-	150	50
	Wireless N Speed	Технология «Эн Спид»	2,4	-	270	50-80
	Wireless N, 300Mbps	Стандарт «Эн 300»	2,4	2006	300	50-120
	Wireless Dual Band N	Стандарт «Дуал Бэнд Эн»	2,4 и 5	2009	300	50-120
	Wireless N, 450Mbps	Технология «Эн 450»	2,4/ 2,4 и 5	-	450	-

Частотные каналы:
Существуют 2 частотных диапазона:
- 2,4 ГГц;
- 5ГГц.

Оба частотных диапазона разбиты на частотные каналы. Ширина каждого частотного канала составляет 20МГц (в некоторых источниках — 22МГц для стандарта IEEE 802.11 b).



Центральная частота первого канала — 2412МГц, второго — 2417МГц, третьего — 2422МГц. Все каналы смещены относительного центра предыдущего на 5МГц. Каждый последующий канал не перекрывается с предыдущим на 5МГц. Однако, есть «чистые» или «неперекрывающиеся» частотные каналы с номерами 1, 6, 11 и 14 (для Японии). Эти каналы не перекрываются и не накладываются с соседними, и не могут влиять на соседние сети, созданные другими устройствами. Многие производители выставляют данные частотные каналы в настройках по умолчанию.
Неперекрывающиеся частотные каналы нужны для создания роуминга в сетях WiFi. В частотном диапазоне 5ГГц таких каналов 23.
Роуминг - Для обеспечения перехода мобильных рабочих станций из зоны действия одной точки доступа к другой в многосотовых ситемах предусмотрены специальные процедуры сканирования (активного и пассивного прослушивания эфира) и присоединения (Association), однако строгих спецификаций по реализации роуминга стандарт 802.11 не предусматривает.



Режимы работы оборудования:

- AP - основной режим работы активного WiFi оборудования (Access Point). В данном режиме, устройства (точки доступа WiFi и WiFi роутеры) создают вокруг себя радиопокрытие, находясь в котором, и, обладая устройством, способным работать в режиме AP-client (все без исключения WiFi адаптеры и некоторые модели точек доступа WiFi) можно подключиться к сети WiFi. WiFi роутеры и точки доступа выполняют одни и те же функции — создают радиопокрытие (режим AP), находясь в котором, любое устройство может подключиться к сети в режиме AP-Client. Данные устройства различаются как визуально, так и структурно. У классической точки доступа WiFi имеется только один Ethernet-порт. WiFi роутер — это более функциональное и универсальное устройство домашней WiFi сети или сети небольшого офиса. Точки доступа, имеющие более богатый функционал в плане различных настроек WiFi сети, чаще используются для создания сетей с большими площадями.
- AP-client - Наиболее типичным устройством, работающим в режиме AP-client является WiFi адаптер, хотя некоторые точки доступа также могут работать в этом режиме. WiFi адаптер — это устройство, позволяющее компьютерам, ноутбукам и прочим устройствам подключаться к WiFi сети, созданной другими устройствами, такими как WiFi точки доступа и WiFi роутеры (активное WiFi оборудование, работающее в режиме AP).
- Ad-Hoc позволяет объединить 2 компьютера во временную одноранговую сеть типа «компьютер-компьютер» и организовать обмен данными между ними всего за несколько минут.
- Bridge необходим для объединения по радиосвязи двух удаленных сегментов сетей Ethernet. После объединения двух точек доступа в мост, WiFi сеть, которую они образовали, соединившись в bridge становиться невидимой, что значительно повышает уровень безопасности, защищая сеть от несанкционированного подключения. Альтернативой режиму Bridge может служить схема из двух устройств — на одной стороне схемы устройство с поддержкой режима AP, на другой — точка доступа в режиме AP-client.
- Repeater повышвет уровень сигнала в какой-либо точке сети WiFi и расширяет покрытие уже существующей сети.
- WDS - Данный режим позволяет воссоздать практически любую топологию. WDS бывает нескольких видов: WDS типа «Точка-Точка» (Point-to-Point), WDS типа «Точка-Многоточка» (Point-to-Multi-Point). Комбинация различных типов WDS = любая сетевая топология сети.

Алгоритм CSMA/CA

Carrier Sense Multiple Access With Collision Avoidance
(Carrier sensing multiple access with collision avoidance)
CSMA/CA - множественный доступ с контролем несущей и избеганием коллизий»— это сетевой протокол, в котором:

- используется схема прослушивания несущей волны;
- станция, которая собирается начать передачу, посылает jam signal (сигнал затора);

- после продолжительного ожидания всех станций, которые могут послать jam signal, станция начинает передачу фрейма;
- если во время передачи станция обнаруживает jam signal от другой станции, она останавливает передачу на отрезок времени случайной длины и затем повторяет попытку.
- CSMA/CA — это модификация чистого Carrier Sense Multiple Access (CSMA).
- CSMA/CA отличается от CSMA/CD тем, что коллизиям подвержены не пакеты данных, а только jam-сигналы.

Защита Wi-fi сетей
- В 1997 году вышел первый стандарт IEEE 802.11, безопасность которого, как оказалось, далека от идеала. Простой пароль SSID (Server Set ID) для доступа в локальную сеть по современным меркам нельзя считать защитой, особенно, учитывая факт, что к Wi-Fi не нужно физически подключаться.
- Главной же защитой долгое время являлось использование цифровых ключей шифрования потоков данных с помощью функции Wired Equivalent Privacy (WEP). Сами ключи представляют из себя обыкновенные пароли с длиной от 5 до 13 символов ASCII, что соответствует 40 или 104-разрядному шифрованию на статическом уровне. Как показало время, WEP оказалась не самой надёжной технологией защиты. И, кстати, все основные атаки хакеров пришлись как раз-таки на эпоху внедрения WEP.
- После 2001 года для проводных и беспроводных сетей был внедрён новый стандарт IEEE 802.1X, который использует вариант динамических 128-разрядных ключей шифрования, то есть периодически изменяющихся во времени. Таким образом, пользователи сети работают сеансами, по завершении которых им присылается новый ключ. Например, Windows XP поддерживает данный стандарт, и по умолчанию время одного сеанса равно 30 минутам.
- В конце 2003 года был внедрён стандарт Wi-Fi Protected Access (WPA), который совмещает преимущества динамического обновления ключей IEEE 802.1X с кодированием протокола интеграции временного ключа Temporal Key Integrity Protocol (TKIP), протоколом расширенной аутентификации Extensible Authentication Protocol (EAP) и технологией проверки целостности сообщений Message Integrity Check (MIC).
- Помимо этого, параллельно развивается множество самостоятельных стандартов безопасности от различных разработчиков, в частности, в данном направлении преуспевают Intel и Cisco. В 2004 году появляется WPA2, или 802.11i, — максимально защищённый стандарт.

Технологии защиты
- WEP;
- 802.1X;
- WPA;
- WPA2.

WEP
Эта технология была разработана специально для шифрования потока передаваемых данных в рамках локальной сети.
Данные шифруются ключом с разрядностью от 40 до 104 бит. Но это не целый ключ, а только его статическая составляющая. Для усиления защиты применяется так называемый вектор инициализации Initialization Vector (IV), который предназначен для рандомизации дополнительной части ключа, что обеспечивает различные вариации шифра для разных пакетов данных. Данный вектор является 24-битным. Таким образом, в результате мы получаем общее шифрование с разрядностью от 64 (40+24) до 128 (104+24) бит. Идея очень здравая, поскольку при шифровании мы оперируем и постоянными, и случайно подобранными символами.
Но, как оказалось, взломать такую защиту можно — соответствующие утилиты присутствуют в Интернете (например, AirSnort, WEPcrack).
Основное её слабое место — это вектор инициализации. Поскольку мы говорим о 24 битах, это подразумевает около 16 миллионов комбинаций (2 в 24 степени) — после использования этого количества ключ начинает повторяться. Хакеру необходимо найти эти повторы (от 15 минут до часа для ключа 40 бит) и за секунды взломать остальную

часть ключа. После этого он может входить в сеть как обычный зарегистрированный пользователь

802.1X

IEEE 802.1X — это новый стандарт, который оказался ключевым для развития индустрии беспроводных сетей в целом. За основу взято исправление недостатков технологий безопасности, применяемых в 802.11, в частности, возможность взлома WEP, зависимость от технологий производителя и т. п. 802.1X позволяет подключать в сеть даже PDA-устройства, что позволяет более выгодно использовать саму идею беспроводной связи. С другой стороны, 802.1X и 802.11 являются совместимыми стандартами. В 802.1X применяется тот же алгоритм, что и в WEP, а именно — RC4, но с некоторыми отличиями.

802.1X базируется на протоколе расширенной аутентификации Extensible Authentication Protocol (EAP), протоколе защиты транспортного уровня Transport Layer Security (TLS) и сервере доступа RADIUS (Remote Access Dial-in User Server). Плюс к этому стоит добавить новую организацию работы клиентов сети. После того, как пользователь прошёл этап аутентификации, ему высылается секретный ключ в зашифрованном виде на определённое незначительное время — время действующего на данный момент сеанса. По завершении этого сеанса генерируется новый ключ и опять высылается пользователю. Протокол защиты транспортного уровня TLS обеспечивает взаимную аутентификацию и целостность передачи данных. Все ключи являются 128-разрядными по умолчанию.

WPA

WPA — это временный стандарт, о котором договорились производители оборудования, пока не вступил в силу IEEE 802.11i. По сути, WPA = 802.1X + EAP + TKIP + MIC, где:

- WPA — технология защищённого доступа к беспроводным сетям (Wi-Fi Protected Access),
- EAP — протокол расширенной аутентификации (Extensible Authentication Protocol),
- TKIP — протокол интеграции временного ключа (Temporal Key Integrity Protocol),
- MIC — технология проверки целостности сообщений (Message Integrity Check).

Ключевыми здесь являются новые модули TKIP и MIC. Стандарт TKIP использует автоматически подобранные 128-битные ключи, которые создаются непредсказуемым способом и общее число вариаций которых достигает 500 миллиардов. Сложная иерархическая система алгоритма подбора ключей и динамическая их замена через каждые 10 Кбайт (10 тыс. передаваемых пакетов) делают систему максимально защищённой.

От внешнего проникновения и изменения информации также обороняет технология проверки целостности сообщений (Message Integrity Check). Достаточно сложный математический алгоритм позволяет сверять отправленные в одной точке и полученные в другой данные. Если замечены изменения и результат сравнения не сходится, такие данные считаются ложными и выбрасываются.

Правда, TKIP сейчас не является лучшим в реализации шифрования, поскольку в силу вступают новые алгоритмы, основанные на технологии Advanced Encryption Standard (AES), которая, кстати говоря, уже давно используется в VPN.

WPA2

WPA2 обеспечивает самый высокий уровень защиты данных и контроль доступа в беспроводную сеть для корпоративных (WPA2-Enterprise) и индивидуальных пользователей (WPA2-Personal).

WPA2 (Wireless Protected Access ver. 2.0) – это вторая версия набора алгоритмов и протоколов обеспечивающих защиту данных в беспроводных сетях Wi-Fi. Как предполагается, WPA2 должен существенно повысить защищенность беспроводных сетей Wi-Fi по сравнению с прежними технологиями. Новый стандарт предусматривает, в частности, обязательное использование более мощного алгоритма шифрования AES (Advanced Encryption Standard) и аутентификации 802.1X.

На сегодняшний день для обеспечения надежного механизма безопасности в корпоративной беспроводной сети необходимо (и обязательно) использование

устройств и программного обеспечения с поддержкой WPA2. Предыдущие поколения протоколов - WEP и WPA содержат элементы с недостаточно сильными защитой и алгоритмами шифрования. Более того, для взлома сетей с защитой на основе WEP уже разработаны программы и методики, которые могут быть легко скачаны из сети Интернет и с успехом использованы даже неподготовленными хакерами-новичками. Протоколы WPA2 работают в двух режимах аутентификации: персональном (Personal) и корпоративном (Enterprise). В режиме WPA2-Personal из введенной открытым текстом парольной фразы генерируется 256-разрядный ключ PSK (PreShared Key). Ключ PSK совместно с идентификатором SSID (Service Set Identifier) используются для генерации временных сеансовых ключей PTK (Pairwise Transient Key), для взаимодействия беспроводных устройств. Как и статическому протоколу WEP, протоколу WPA2-Personal присуще определенные проблемы, связанные с необходимостью распределения и поддержки ключей на беспроводных устройствах сети, что делает его более подходящим для применения в небольших сетях из десятка устройств, в то время как для корпоративных сетей оптимален WPA2-Enterprise .
В режиме WPA2-Enterprise решаются проблемы, касающиеся распределения статических ключей и управления ими, а его интеграция с большинством корпоративных сервисов аутентификации обеспечивает контроль доступа на основе учетных записей. Для работы в этом режиме требуются такие регистрационные данные, как имя и пароль пользователя, сертификат безопасности или одноразовый пароль, аутентификация же осуществляется между рабочей станцией и центральным сервером аутентификации. Точка доступа или беспроводной контроллер проводят мониторинг подключений и направляют аутентификационные запросы на соответствующий сервер аутентификации (как правило, это сервер RADIUS, например Cisco ACS). Базой для режима WPA2-Enterprise служит стандарт 802.1X, поддерживающий аутентификацию пользователей и устройств, пригодную как для проводных коммутаторов, так и для беспроводных точек доступа.

Литература:

- Лекции Береснева