СЛУЧАЙНЫЕ МЕТОДЫ ДОСТУПА К МОНОКАНАЛУ

6.0.1.1

Различные алгоритмы доступа к моноканалу разрабатывают по причине необходимости разрешения конфликтов между станциями при взаимодействии посредством разделяемой СрПД.

6.0.1.2

В первую очередь затрагиваются передатчики, то есть активные компоненты системы. Проблема заключается в «столкновениях» конкурирующих передатчиков.

Пассивные по своей природе приемники априори конфликтовать не могут. Хотя количество приемников всегда ограничивается, так как передатчики имеют конечную нагрузочную способность.

Если находящиеся в равных условиях два либо более передатчиков одновременно выдают сигналы в СрПД (например, устанавливают соответствующие уровни напряжения), то возникает противоречие. Таковое единовременно неразрешимое противоречие принято называть *коллизией* (collision).

6.0.1.3

Коллизия может быть как логической (информационный конфликт) так и физической (несовместимые физические процессы).

Обычно коллизия возникает при попытках установить противоположные логические уровни.

Кроме всего прочего, физическая коллизия чревата выходом из строя передатчиков, даже при попытках установить одинаковые логические уровни, так как многие среды не допускают наличие более чем одного активного усилителя сигнала без применения специальных схемотехнических решений.

Классическим способом защиты оборудования от коллизий является так называемая гальваническая развязка (трансформаторная либо оптронная).

При попытках установить разные уровни, как правило, наблюдаются эффекты «зануления» и «заединичивания» -- в зависимости от особенностей элементной базы.

6.0.1.4

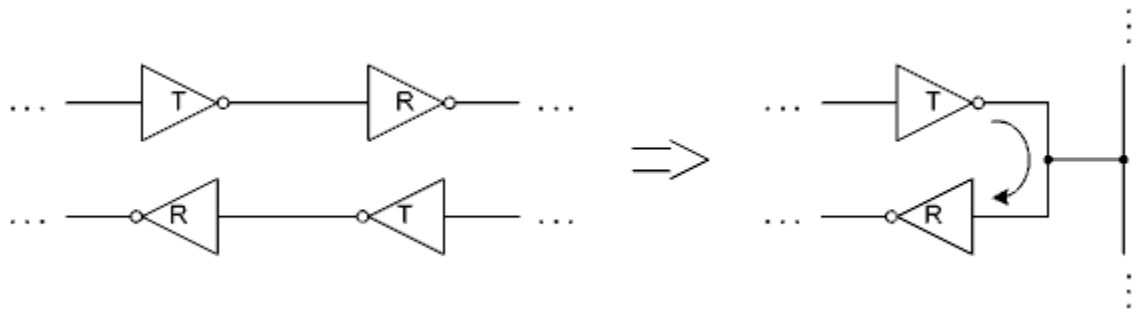
Ситуация с коллизией может затрагивать только станции, подключенные к одной СрПД, то есть сегмент компьютерной сети.

Сегмент, в котором возможно возникновение коллизий называется *доменом коллизий* (collision domain).

Понятие коллизии относится не только к сигналу, а и к пакету.

Чтобы передатчик мог бороться с коллизиями он безусловно должен иметь возможность определять факт их наличия.

Борьба с коллизиями, по определению, актуальна применительно к многоточечным топологиям (если под точками понимать подключения), типичными представителями которых являются шинная топология и эфир. На практике, при переходе от двухточечной топологии к многоточечной цепи передатчика и приемника всегда совмещаются.



Получить легко наращиваемую структуру по-другому невозможно.

6.0.1.5b

Ответ на вопрос о том как передатчик определяет наличие коллизии весьма удачно «заложен» в показанную схемотехнику. Можно легко заметить, что любая переданная передатчиком порция данных, например байт, тут же будет принята приемником. Достаточно просто сравнить (аппаратно или программно) байт до передачи с байтом после приема. Несовпадение свидетельствует о том, что была коллизия. Ну а если вдруг даже после коллизии данные совпали, то это «устраивает все стороны».

6.0.1.6

Физические свойства СрПД не позволяют мгновенно передавать сигналы. Следовательно и возникшая коллизия распространяется по сегменту с конечной скоростью.

Под *окном коллизий* (collision window) понимается временной интервал, в течение которого любая из станций гарантированно обнаруживает коллизию, равный удвоенному времени прохождения сигнала между двумя максимально удаленными станциями.

Без учета окна коллизий, влияющего на время постудержания сигнала, невозможно спроектировать работоспособный сегмент.

6.0.1.7

Почему окно коллизий равно удвоенному времени прохождения сигнала между двумя максимально удаленными станциями?

6.0.2.1

Существуют два основных подхода к проблеме коллизий:

1. Не допускать коллизии вообще, то есть пользоваться детерминированными методами доступа к моноканалу.

2. Допускать коллизии и каким-то образом выходить из них, что достижимо только использованием случайных методов доступа к моноканалу.

Во втором случае так же можно выделить два подхода:

1. Не обращать внимание на причины возникновения коллизий, а упор делать на способ выхода из них.

2. Пытаться предотвращать коллизии тем самым максимально снижая их количество, ну а если коллизии все-таки возникают, то «тяжело» выходить из них.

Таким образом, все методы доступа к моноканалу делят на:

1. *Случайные* (contention-based).

2. *Детерминированные* (controlled).

6.0.2.2

Все случайные методы основаны на использовании генератора случайных чисел (поэтому их так и называют), который позволяет делать случайные задержки при доступе к моноканалу, а значит и с определенной степенью вероятности избегать коллизии.

6.0.2.3

На эффективность случайных методов наиболее существенное влияние оказывают следующие факторы:

-- количество взаимодействующих станций;

-- инертность среды передачи данных;

-- длина кадра;

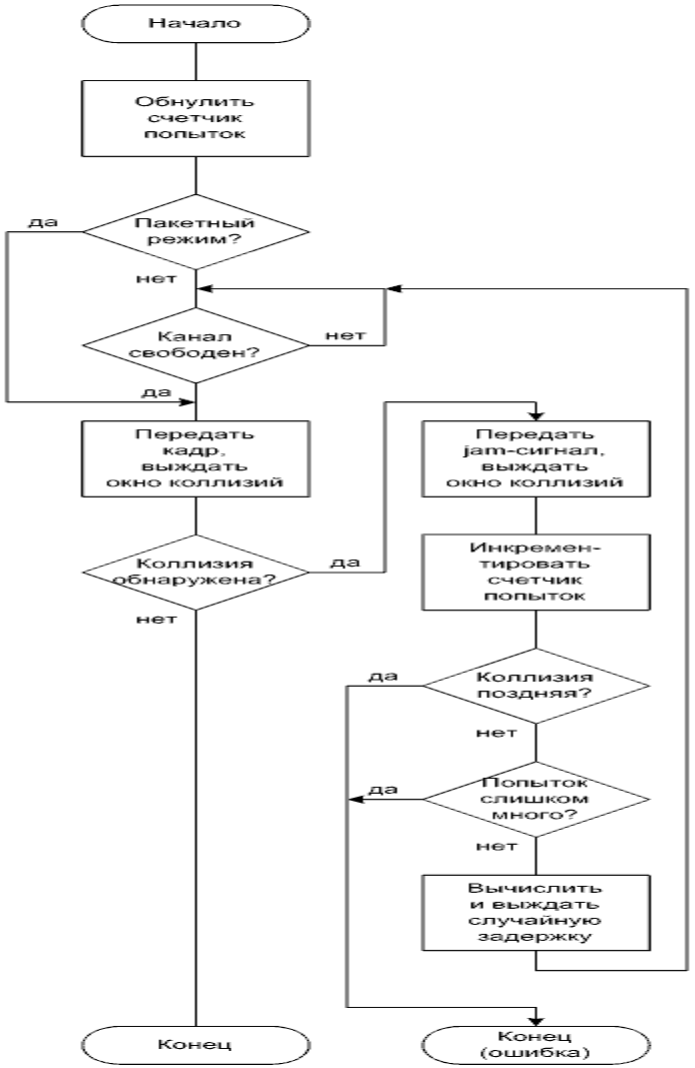
-- частота синхронизации.

6.0.2.4

Назовите основные достоинства случайных методов доступа.
Назовите основные недостатки случайных методов доступа.

6.0.3.1

С точки зрения изучения случайных методов доступа к моноканалу наиболее наглядным примером является классический алгоритм CSMA/CD (Carrier Sense Multiple Access with Collision Detection) -- множественный доступ с прослушиванием несущей и обнаружением коллизий, описанный в стандарте Ethernet (IEEE 802.3).



Алгоритм CSMA/CD. Передача очередного кадра

6.0.3.3

Алгоритм CSMA/CD. Прием очередного кадра

6.0.3.4

Задержка перед началом очередной попытки передачи после коллизии (backoff) измеряется в так называемых слот-таймах, количество которых является случайным целым числом *r*:

$0 \le r \le 2^k$,

где

$k = \min(n, 10)$,

где *n* -- номер попытки.

После превышения счетчиком попыток некоторого порогового значения дальнейшие попытки считаются бесперспективными.

Значение *k* не может быть больше 10.

6.0.3.5

Качество диспетчеризации при обработке коллизий по большому счету зависит от одного базового параметра.

Слот-тайм (slot time) является минимальной неделимой единицей времени при диспетчеризации и подбирается с учетом многих других параметров. По крайней мере, он должен быть больше суммы удвоенного времени прохождения сигнала по сегменту и времени передачи jam-сигнала.

6.0.3.6

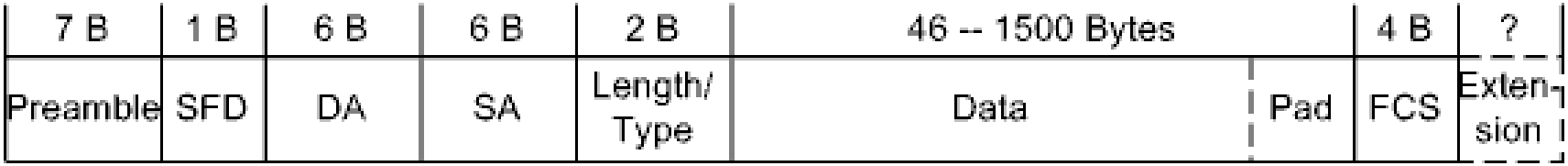
Назовите две причины, по которым нужен jam-сигнал.

6.0.3.7

В стандарт заложен механизм ускорения распределенного обнаружения коллизий, заключающийся в их «усилении».

Каждая обнаружившая коллизию станция передает специальный *jam-сигнал* некоторой длительности (значение стандартом не регламентируется).

Jam-сигнал выполняет две важные функции. Во-первых, является признаком возникновения коллизии, что позволяет другим станциям сразу «увидеть» коллизию (столкнувшиеся передатчики, выставившие jam-сигнал, и так знают о коллизии). Во-вторых, позволяет синхронизировать время начала отсчетов случайных задержек.



Поля:
Preamble -- преамбула.
SFD (Start Frame Delimiter) -- разграничитель начала кадра.
DA (Destination Address) -- адрес назначения.
SA (Source Address) -- адрес источника.
Length/Type -- длина либо тип.
Data -- данные.
Pad -- наполнитель.
FCS (Frame Check Sequence) -- контрольная сумма.
Extension -- расширитель.

Формат кадра Ethernet

6.0.3.9

Предусмотрены полудуплексный и полнодуплексный режимы, «поведение» в которых несколько различается.

В качестве преамбулы выступают семь байтов со значением 10101010b, а в качестве SFD -- байт со значением 10101011b.

При сборке кадра учитываются ограничения на его длину. Ограничивается не только максимальная длина, а и минимальная.

При недостаче в поле данных вслед за ним в кадр вставляются дополнительные октеты-наполнители (значения стандартом не регламентируются).

Параметр MTU (Maximum Transmission Unit) определяет максимальный размер вкладываемых данных. Применительно к Ethernet, если значение поля Length/Type больше либо равно 1536 (600h), то указывает тип инкапсулируемых данных.

При необходимости, октеты-расширители дополняет кадр до тайм-слота (только в полудуплексном режиме).

6.0.3.10

Ethernet-заголовок имеет фиксированную длину.

Но, поскольку многие базирующиеся на Ethernet технологии (например, виланы) имеют собственные подзаголовки, заголовок, а следовательно и весь кадр, может увеличиться, правда незначительно и не затрагивая MTU (такие кадры иногда называют baby giant).

Некоторые технологии предусматривают значительное увеличение кадра уже за счет увеличения MTU. Например, параметр MTU технологии FCoE (Fibre Channel over Ethernet) равен 2500 байтам (такие кадры иногда называют mini jumbo).

Наконец, многие производители оборудования Ethernet предусмотрели нестандартное (но в большинстве случаев совместимое) административное увеличение MTU вплоть до 9000 байтов -- в первую очередь, для оптимизации пересылки больших объемов данных. Такие Ethernet-кадры называют *гигантскими* (jumbo).

6.0.3.11

В качестве контрольного кода используется код CRC.

6.0.3.12

При функционировании с пропускной способностью выше 100 Mbit/s (только в полудуплексном режиме) реализация может опционально передавать серию кадров ослабив контроль среды.

Такой режим работы называется *пакетным режимом* (burst mode).

Сразу после успешной передачи первого кадра начинается безусловная передача последующих кадров -- это возможно, поскольку передатчики других станций по-прежнему будут находиться в состоянии ожидания.

Интервалы между кадрами (interframe gaps), без которых принимающая станция вообще не сможет различать кадры, укорочены до минимума с помощью октетов-расширителей.

Количество кадров в пакете ограничивается.

Считается, что в правильно сконфигурированном сегменте при передаче второго и последующих кадров пакета коллизии возникать не должны. Однако, если такая коллизия возникает, то она обрабатывается особо (выход из алгоритма с ошибкой) -- это так называемая поздняя коллизия (late collision).

6.0.3.13

Parameters	Values
slotTime	512 bit times
interFrameGap	96 μs
attemptLimit	16
backoffLimit	10
jamSize	32 bits
maxFrameSize	1518 octets
minFrameSize	512 bits (64 octets)
burstLimit	not applicable

Parameters	Values
slotTime	512 bit times
interFrameGap	0.96 µs
attemptLimit	16
backoffLimit	10
jamSize	32 bits
maxUntaggedFrameSize	1518 octets
minFrameSize	512 bits (64 octets)
burstLimit	not applicable

Parameters	Values
slotTime	4096 bit times
interFrameGap	0.096 µs
attemptLimit	16
backoffLimit	10
jamSize	32 bits
maxUntaggedFrameSize	1518 octets
minFrameSize	512 bits (64 octets)
burstLimit	65 536 bits

Примеры значений параметров Ethernet (10, 100, 1000 Mbit/s соответственно) [IEEE]

6.0.4.1

Еще одним примером случайных методов доступа к моноканалу является гораздо более сложный алгоритм CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) -- множественный доступ с прослушиванием несущей и избеганием коллизий, описанный в стандарте Wi-Fi (IEEE 802.11).

6.0.4.2a

Для понимания алгоритма необходимо ввести термины из стандарта.

Применительно к Wi-Fi, MAC-подуровень канального уровня поделен еще на два слоя.

На нижнем слое расположен только один блок под названием DCF (Distributed Coordination Function) -- функционал распределенного координируемого взаимодействия. DCF и составляет ядро алгоритма CSMA/CA. Все станции сегмента должны поддерживать DCF.

Над DCF расположены:

1. PCF (Point Coordination Function) -- функционал координируемого взаимодействия с использованием станции-координатора.
2. HCF (Hybrid Coordination Function) -- функционал гибридного координируемого взаимодействия.
3. MCF (Mesh Coordination Function) -- функционал сеточного координируемого взаимодействия.

Из них формируются следующие опциональные блоки:

1. PCF.
2. HCCA (HCF Controlled Access).
3. EDCA (HCF/MCF Contention Access).
4. MCCA (MCF Controlled Access).

Кроме DCF, наибольший интерес представляет PCF. Остальные блоки предназначены для поддержки QoS.

6.0.4.3

В настоящее время реализации Wi-Fi на физическом уровне (беспроводные) очень разнообразны -- используются до десяти различных способов модуляции.

Более того, для Wi-Fi характерно создание большого числа параллельных каналов.

6.0.4.4

Стандартом предусмотрены целых шесть вариантов отслеживаемых межкадровых интервалов -- IFSes (InterFrame Spaces):

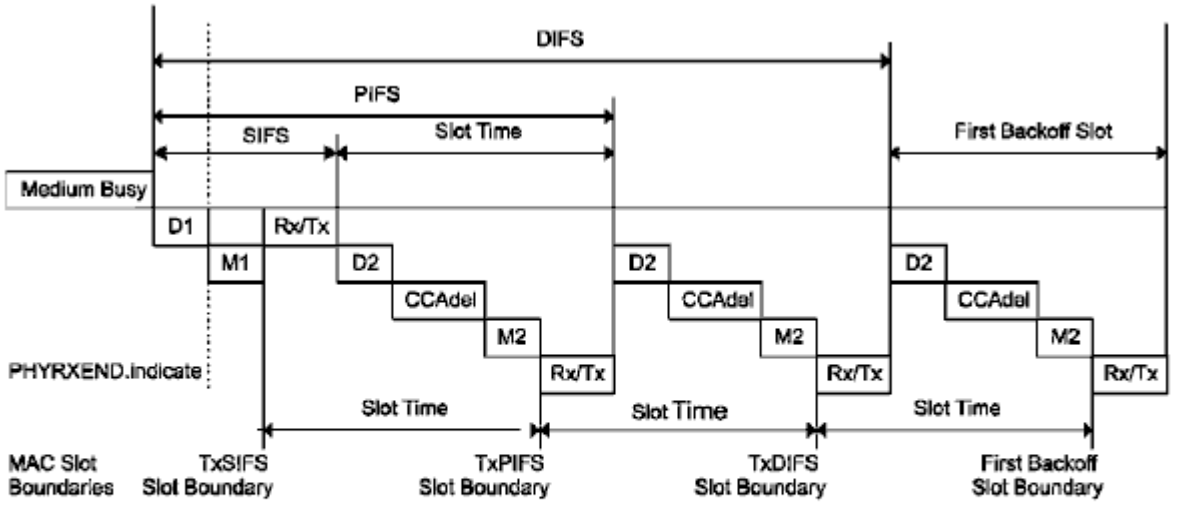
1. RIFS (Reduced IFS) -- сокращенный.
2. SIFS (Short IFS) -- короткий.
3. PIFS (PCF IFS) -- для PCF.
4. DIFS (DCF IFS) -- для DCF.
5. AIFS (Arbitration IFS) -- для QoS-арбитража.
6. EIFS (Extended IFS) -- расширенный.

6.0.4.5

Для чего может понадобиться вводить разные IFSes?

Отслеживание различных IFSes в различных ситуациях влияет на способность станции «видеть щели» между кадрами, а значит и на способность «вклиниваться» в пересылку.

IFSes рассчитывают на основании комплекса параметров.



D1 = aRxRFDelay + aRxPLCPDelay (referenced from the end of the last symbol of a frame on the medium)
D2 = D1 + Air Propagation Time
Rx/Tx = aRXTXTurnaroundTime (begins with a PHYTXSTART.request)
M1 = M2 = aMACProcessingDelay
CCAdel = aCCA Time - D1

Кроме интервала DIFS, используемого функционалом DCF, наиболее интересны SIFS и PIFS.

Случайная задержка измеряется в слот-таймах, как и в Ethernet, но алгоритм другой. Количество слот-таймов является случайным целым числом *Random*:

$$0 \le Random \le CW ,$$

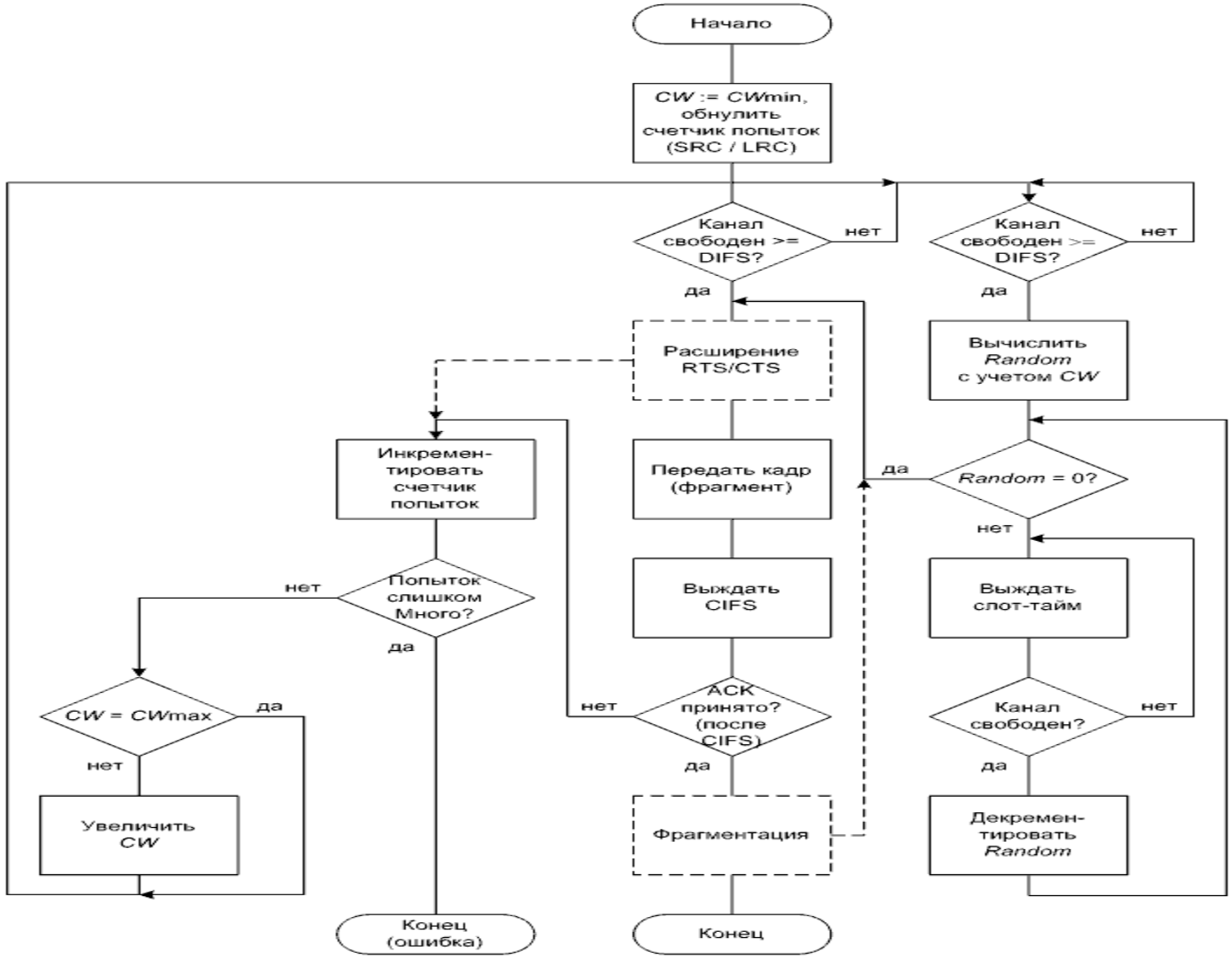
где *CW* (contention window) -- так называемое окно состязаний:

$$CW_{min} \le CW \le CW_{max} ,$$

и берется из ряда: 7, 15, 31 ... (два в некоторой степени минус один).

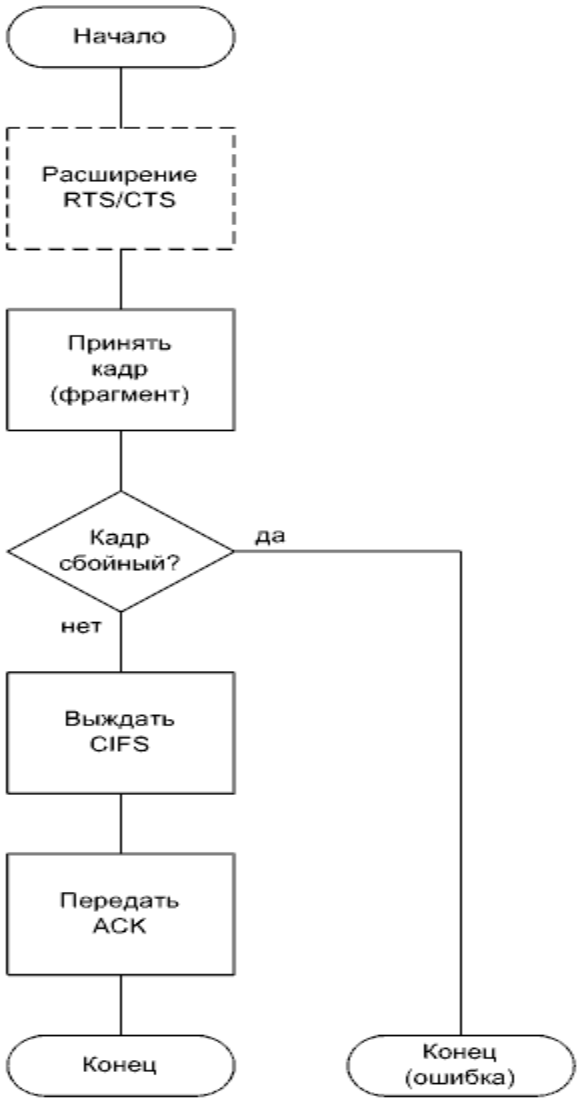
Крайние значения зависят от способа модуляции (типичное значение CW_{min} -- 15, типичное значение CW_{max} -- 1023).

Предусмотрены два счетчика попыток: SRC (Short Retry Count) и LRC (Long Retry Count). Количество попыток ограничивается. Выбор значения зависит от физического уровня.



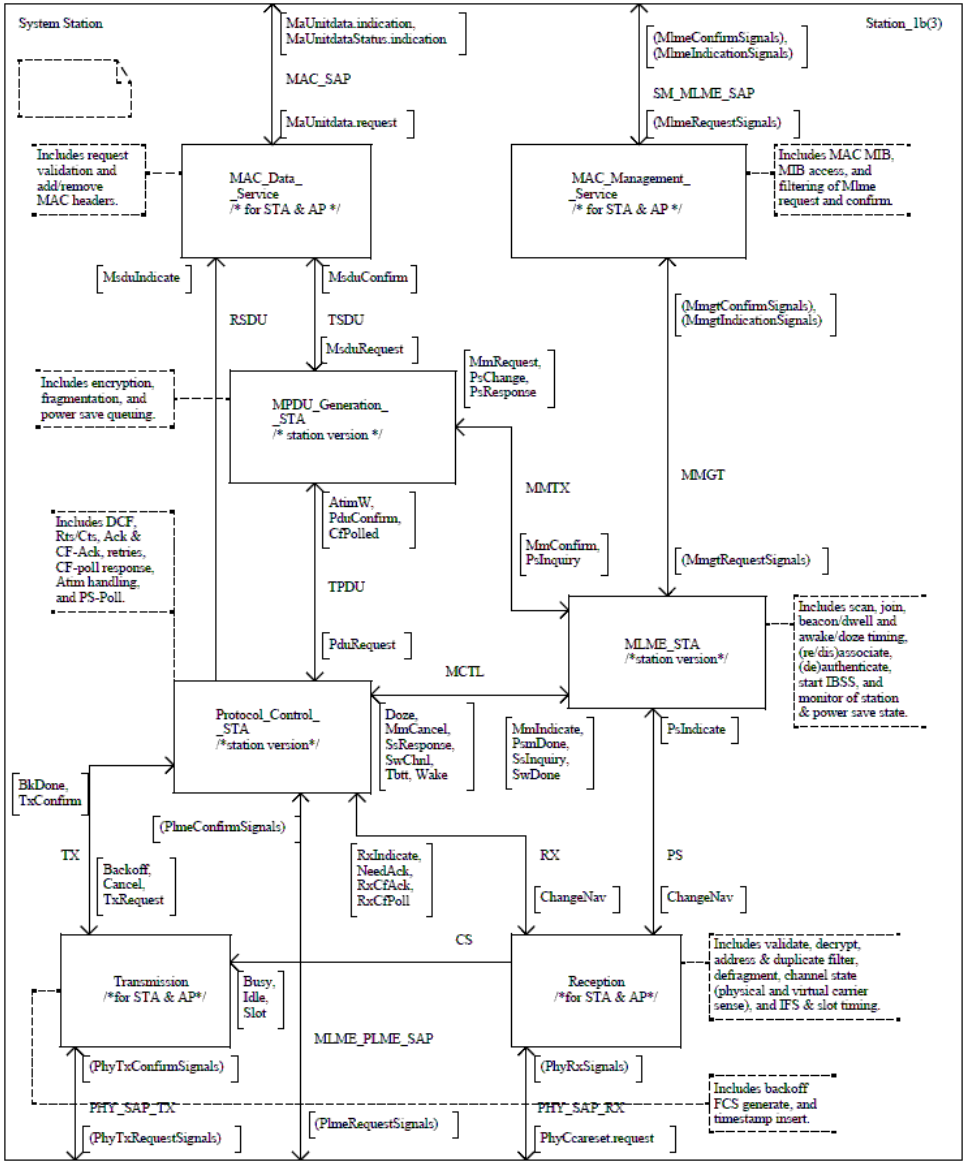
Очень упрощенный алгоритм CSMA/CA (Wi-Fi). Передача очередного кадра

6.0.4.9



Очень упрощенный алгоритм CSMA/CA (Wi-Fi). Прием очередного кадра

6.0.4.10



Фрагмент полного алгоритма Wi-Fi (одна страница из 192) [IEEE]

6.0.4.11

Для беспроводных каналов свойственны две проблемы, которые получили следующие названия:

1. Hidden node problem -- проблема скрытой станции.

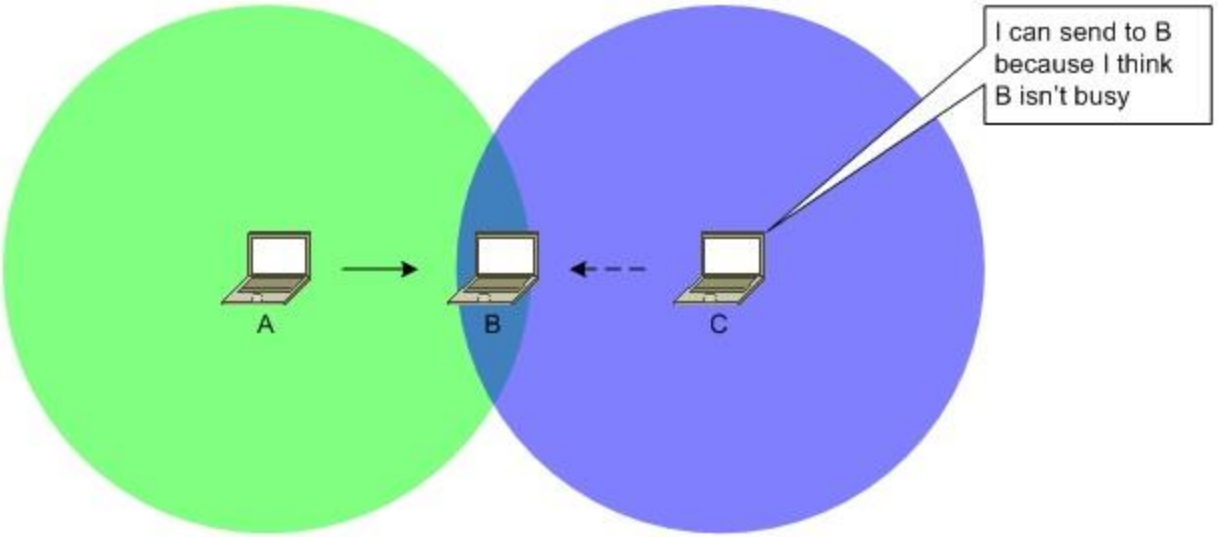
2. Exposed node problem -- проблема доступной станции.

Предполагается, что все станции взаимодействуют в рамках одного канала.

(Эти проблемы возникнут и в проводных каналах, если не учесть окно коллизий.)

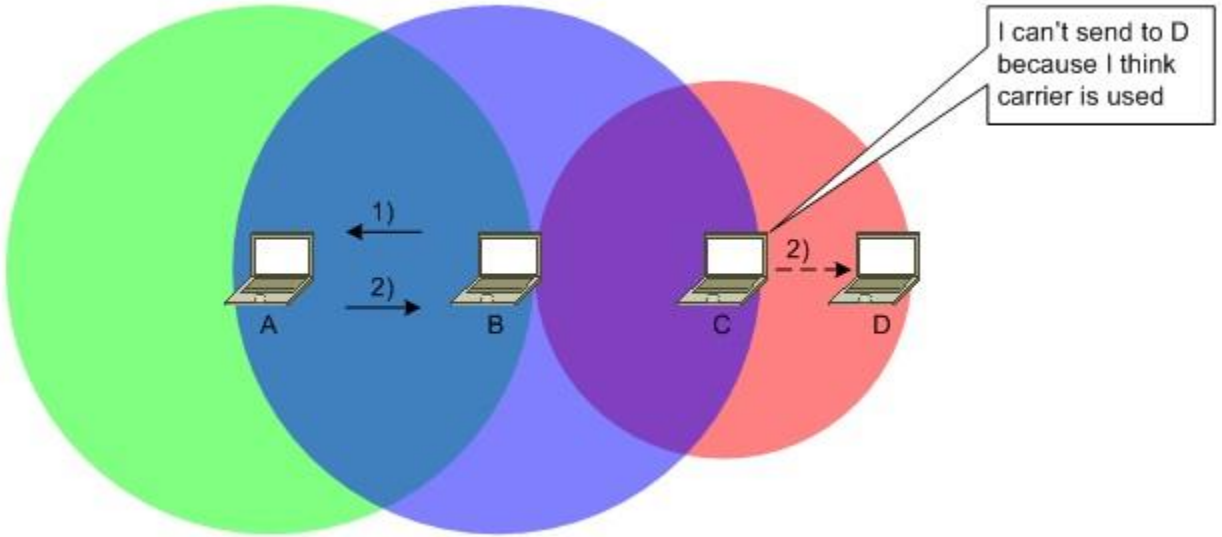
6.0.4.12

Проблему скрытой станции можно сформулировать так: станция С может ошибочно начать передачу станции В, так как не может «услышать» что станция А уже передает станции В (станция А «скрыта» от станции С).



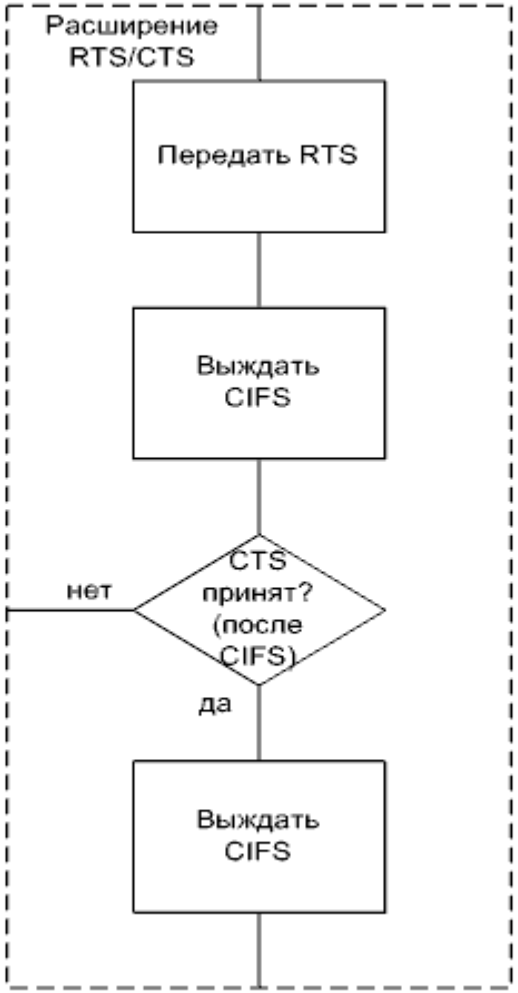
6.0.4.13

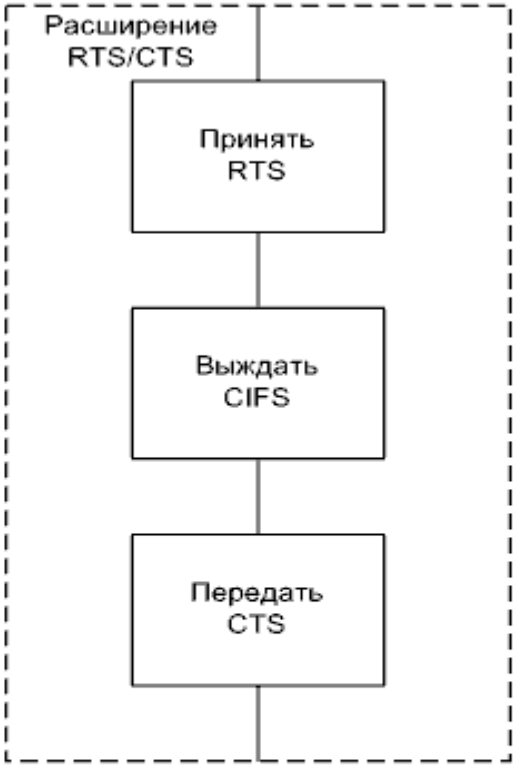
Проблему доступной станции можно сформулировать так: станция C, зная о взаимодействии станций A и B, не может передать станции D во время пассивности станции B, а могла бы, поскольку считает канал занятым ошибочно (станция C «доступна» для станции D).



6.0.4.14

Частично решить проблемы помогает опциональное расширение RTS/CTS.





Алгоритм CSMA/CA (Wi-Fi). Расширение RTS/CTS

6.0.4.16

Кадры, поступившие на канальный уровень для дальнейшей передачи, называются MSDUs (MAC Service Data Units) и могут быть размером до 2304 байтов.

MSDUs разбиваются на меньшие фрагменты, называемые MPDUs (MAC Protocol Data Units), которые передаются в пакетном режиме. Длина фрагментов также ограничивается (например, 4095 байтов).

Уменьшение длины фрагментов приводит к уменьшению вероятности коллизии при передаче отдельно взятого фрагмента, но и к увеличению количества фрагментов.

Алгоритм CSMA/CA (Wi-Fi). Фрагментация

6.0.4.18

Еще одним механизмом Wi-Fi для предотвращения коллизий является резервирование канала.

Все станции в сегменте обязаны иметь таймеры, называемые NAVs (Network Allocation Vectors). Каждый раз при резервировании значение таймера обновляется согласно временно'му интервалу резервирования и затем уменьшается.

Станция не имеет права начать передачу до тех пор, пока значение не достигнет нуля (плюс DIFS).

Обращение к таймеру при необходимости передать кадр, в терминологии Wi-Fi, называется виртуальным прослушиванием несущей (происходит параллельно с физическим прослушиванием).

Несмотря на все описанные меры, вероятность коллизий все-равно не равна нулю.

В связи с особенностями беспроводных каналов, в них передатчикам значительно сложнее самостоятельно обнаруживать коллизии. Поэтому эта функция с них снимается и возлагается на приемники.

Вместо обнаружения коллизии, передатчик ждет положительное подтверждение ACK от приемника. Коллизия, как и любая другая проблема с кадром, приведет к отсутствию подтверждения и, далее, к повторной передаче.

6.0.4.20a

Формат кадра Wi-Fi так же сло'жен -- в сравнении с форматом кадра Ethernet. При этом наличие и названия последующих полей зависит от значения предыдущих.

2 Bytes	2 B	6 B	6 B	6 B	2 B	6 B	2 B	4 B	0 -- 7951 B	4 B
Frame Control	Duration /ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	QoS Control	HT Control	Data	FCS

Header

2 bits	2 b	4 b	1 b	1 b	1 b	1 b	1 b	1 b	1 b	1 b
Protocol Version	Type	Subtype	To DS	From DS	More Fragments	Retry	Power Management	More Data	Protected Frame	Order

Обобщенный формат кадра Wi-Fi

Поля:

1. Frame Control -- контроль кадра.
2. Duration/ID -- длительность-идентификатор (0 -- 32767 us при резервировании канала, трактовка зависит например от наличия QoS).
3. Address 1 -- адрес 1.
4. Address 2 -- адрес 2.
5. Address 3 -- адрес 3.
6. Sequence Control -- контроль последовательности.
7. Address 4 -- адрес 4.
8. QoS Control -- контроль QoS.
9. HT Control (High Throughput) -- контроль интенсивной пересылки (при QoS).
10. Frame Body -- содержимое кадра (данные).
11. FCS (Frame Control Sequence) -- контрольная сумма.

6.0.4.20c

Поля контроля кадра:

1. Protocol Version -- версия протокола (до сих пор равна нулю).

2. Type -- тип: 00 -- Management -- управление, 01 -- Control -- контроль 10 -- Data -- данные, 11 -- Reserved -- зарезервировано.

3. Subtype -- подтип (в настоящее время определено около сорока подтипов).

4. To DS -- флаг направления в распределительную систему (проводную систему, связывающую беспроводные сегменты).

5. From DS -- флаг направления из распределительной системы.

6. More Fragments -- флаг наличия фрагментации.

7. Retry -- флаг повторной попытки передачи.

8. Power Management -- флаг режима энергосбережения.

9. More Data -- флаг наличия дополнительных данных (например, буферизированных данных для находящейся в режиме энергосбережения станции).

10. Protected Frame -- флаг защищенности кадра (шифрования).

11. Order -- флаг упорядоченности (при QoS).

Таким образом, существуют три типа кадров.

6.0.4.20d

В зависимости от подтипа кадра в адресных полях могут комбинироваться до четырех из пяти возможных адресов:

BSSID (Basic Service Set Identifier) -- идентификатор так называемой базовой зоны обслуживания (то есть беспроводного сегмента),

SA (Source Address) -- адрес источника,

DA (Destination Address) -- адрес назначения,

TA (Transmitting station Address) -- адрес станции-передатчика (непосредственного),

RA (Receiving station Address) -- адрес станции-приемника (непосредственного).

Table Valid type and subtype combinations

Type value b3 b2	Type description	Subtype value b7 b6 b5 b4	Subtype description
00	Management	0000	Association request
00	Management	0001	Association response
00	Management	0010	Reassociation request
00	Management	0011	Reassociation response
00	Management	0100	Probe request
00	Management	0101	Probe response
00	Management	0110	Timing Advertisement
00	Management	0111	Reserved
00	Management	1000	Beacon
00	Management	1001	ATIM
00	Management	1010	Disassociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication
00	Management	1101	Action
00	Management	1110	Action No Ack
00	Management	1111	Reserved
01	Control	0000–0110	Reserved
01	Control	0111	Control Wrapper
01	Control	1000	Block Ack Request (BlockAckReq)
01	Control	1001	Block Ack (BlockAck)
01	Control	1010	PS-Poll
01	Control	1011	RTS
01	Control	1100	CTS
01	Control	1101	ACK
01	Control	1110	CF-End
01	Control	1111	CF-End + CF-Ack
10	Data	0000	Data
10	Data	0001	Data + CF-Ack
10	Data	0010	Data + CF-Poll
10	Data	0011	Data + CF-Ack + CF-Poll
10	Data	0100	Null (no data)
10	Data	0101	CF-Ack (no data)
10	Data	0110	CF-Poll (no data)
10	Data	0111	CF-Ack + CF-Poll (no data)
10	Data	1000	QoS Data
10	Data	1001	QoS Data + CF-Ack
10	Data	1010	QoS Data + CF-Poll
10	Data	1011	QoS Data + CF-Ack + CF-Poll
10	Data	1100	QoS Null (no data)
10	Data	1101	Reserved
10	Data	1110	QoS CF-Poll (no data)
10	Data	1111	QoS CF-Ack + CF-Poll (no data)
11	Reserved	0000–1111	Reserved

Типы и подтипы кадров Wi-Fi [IEEE]

6.0.4.22

При PCF, «привязка» оконечной станции к станции-координатору (так называемой точке доступа) протекает в три фазы:

1. Discovery -- обнаружение.
2. Authentication -- аутентификация.
3. Association -- ассоциирование.

6.0.4.23

Обнаружение может быть активным -- станция-координатор периодически извещает о себе и своих услугах с помощью кадров-«маяков» (beacons), и пассивным -- станция-координатор отвечает на кадры-«пробы» со стороны оконечных станций (probe requests и probe responses).

6.0.4.24

В рамках CSMA/CA существуют две группы алгоритмов:

1. Без наличия станции-координатора и с упреждающим jam-сигналом.
2. С наличием станции-координатора.

6.0.5.1

Кроме Ethernet и Wi-Fi, в список существующих реализаций случайных методов следует включить технологию Aloha с одноименным алгоритмом.

Эта технология была разработана в университете Гавайских островов и была одной из самых ранних технологий КС.

В виде стандарта так и не была утверждена.

Нашла лишь ограниченное применение в беспроводных каналах для подключения мобильных телефонов первого поколения. Уже давно считается устаревшей.

Скорость: меньше 1 Mbit/s.

Логическая топология: двунаправленное кольцо с разделенными цепями передатчиков и приемников.

Физическая топология: звезда. Требовалось дополнительное сетевое оборудование (концентраторы).

Алгоритм представлял собой сильно упрощенный вариант алгоритма Ethernet. Позже был немного усовершенствован и получил название Slotted Aloha.