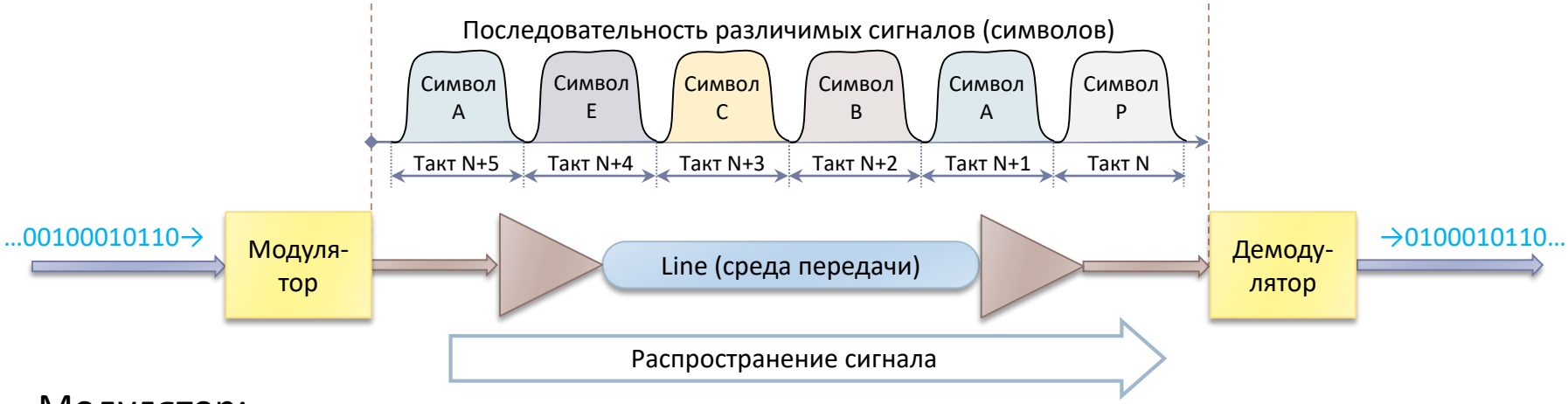
Архитектура компьютерных сетей

Останков Александр Иванович

План курса

1. Введение в компьютерные сети
2. Основные методы построения СПД
3. Архитектура Internet Protocol Suite (TCP/IP)
4. **Архитектура модулей физического уровня**
    - 4.1. Дискретный канал связи
    - 4.2. Среды передачи сигналов и их свойства
    - 4.3. Скорость передачи данных по дискретному каналу
5. Технологии беспроводных сетей
6. Архитектура модулей канального уровня
7. Протоколы транспортного уровня
8. Технологии WWW

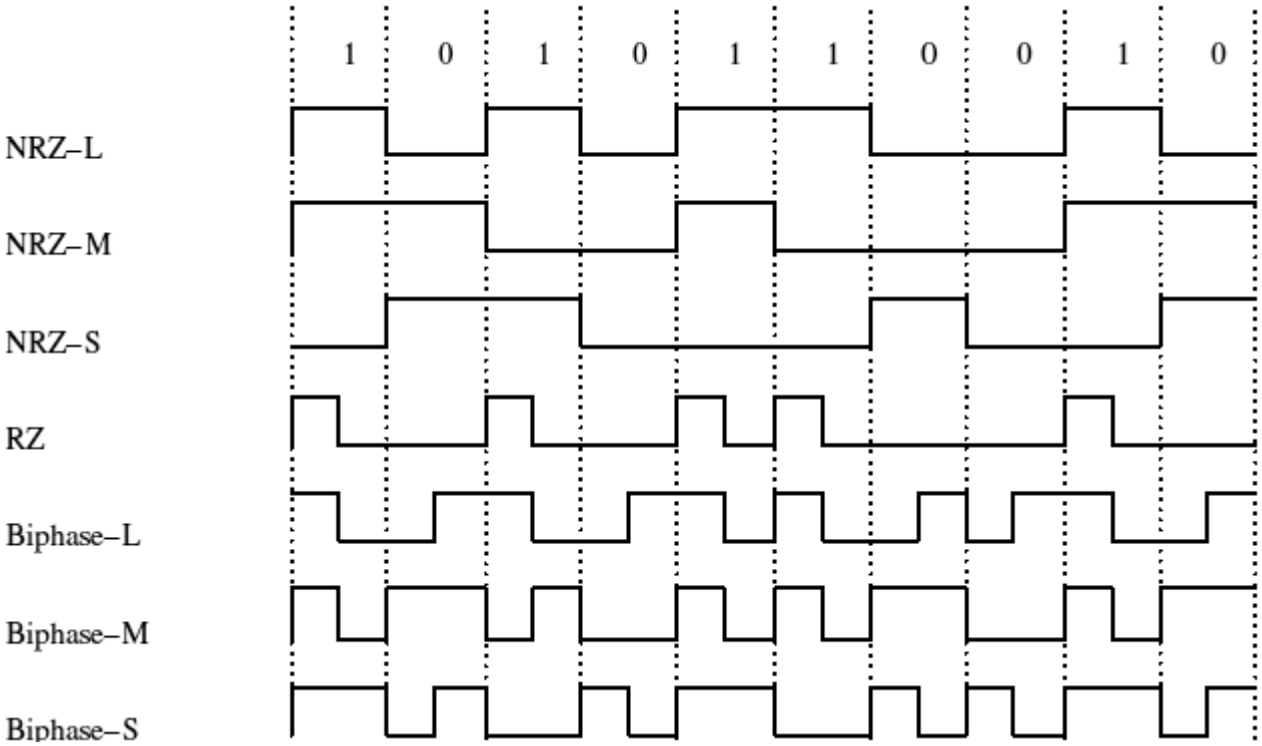
Устройство дискретного канала передачи



Модулятор:

- Генерирует последовательность символов одинаковой длительности T_s
- Каждый символ это различимый сигнал из известного алфавита $S_1 \ldots S_k$
- Частота формирования символов модулятором обычно фиксирована и называется частотой манипуляции $V_m = 1/T_s$ [измеряется в Бодах]
- Если размер алфавита $K > 2$, то каждый символ может кодировать несколько бит входной информации $E = \log_2(K)$, таким образом скорость передачи такого канала будет составлять $V = V_m \cdot \log_2(K)$ [бит/сек]
- обычно размер алфавита K выбирается 2^m (или чуть больше), тогда каждый символ кодирует группу из m входных битов

Способы простейшего линейного кодирования



уровень – 0 или 1

1(mark) – смена уровня

0(space) – смена уровня

единичные импульсы с возвратом

перепад в центре 0-/, 1-\

1(mark) - перепад в центре

0(space) - перепад в центре

Как достичь высокой скорости передачи

$$V = V_m \cdot log_2(K) \quad [\text{бит/сек}]$$

Общая скорость передачи по каналу будет возрастать, если

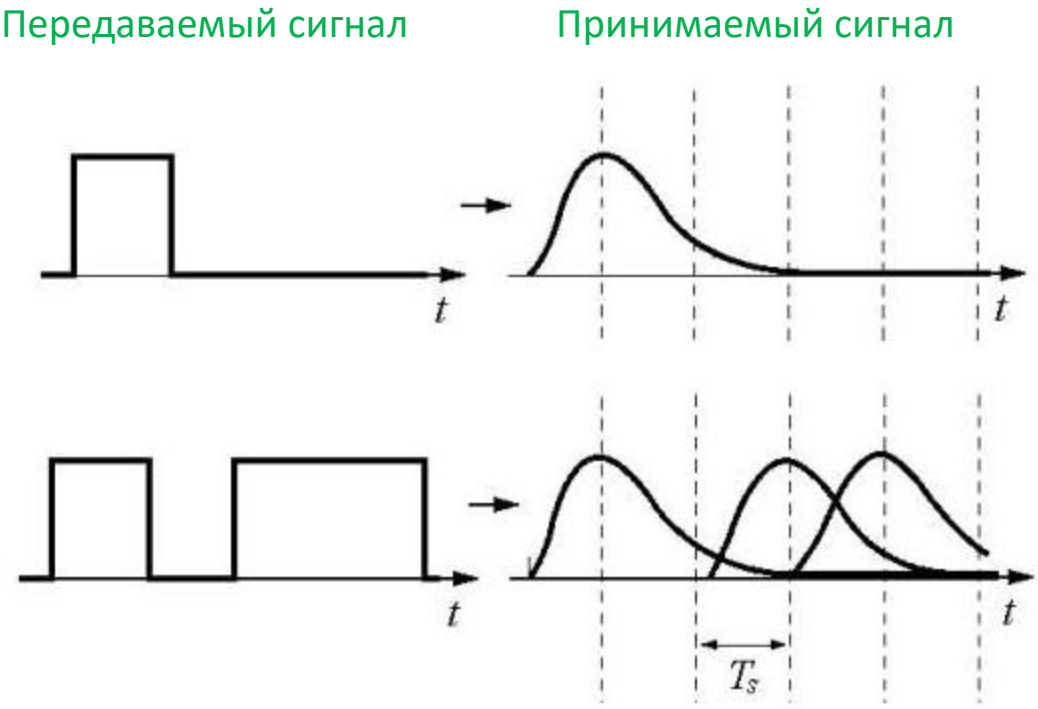
1. Увеличивать частоту манипуляции V_m
2. Увеличивать размер алфавита K

Однако физические свойства реальных сред передачи ограничивают возможности по увеличению общей скорости из-за неизбежного наличия искажений сигнала:

- Искажения спектра
- Шум (помехи)

В результате их действия форма принимаемого сигнала может так сильно исказиться, что в результате приёмник будет не в состоянии распознавать символы в принимаемом сигнале. Очевидно, что передача данных по такому каналу будет невозможна.

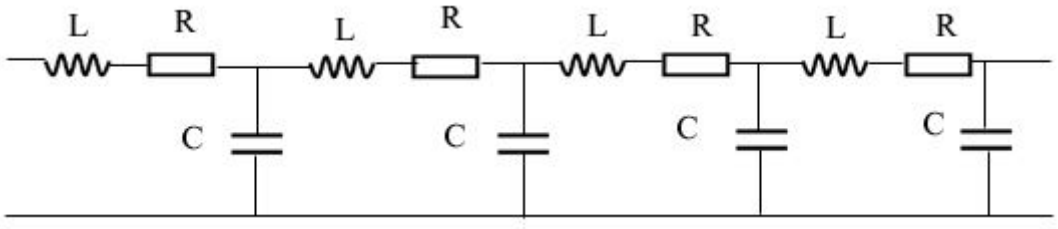
Межсимвольная интерференция



В достаточно длинных линиях происходит специфическое искажение формы импульсов, приводящее к их «расширению». В результате импульсы из соседних тактов могут начать влиять друг на друга - интерферировать, вплоть до потери возможности их различения

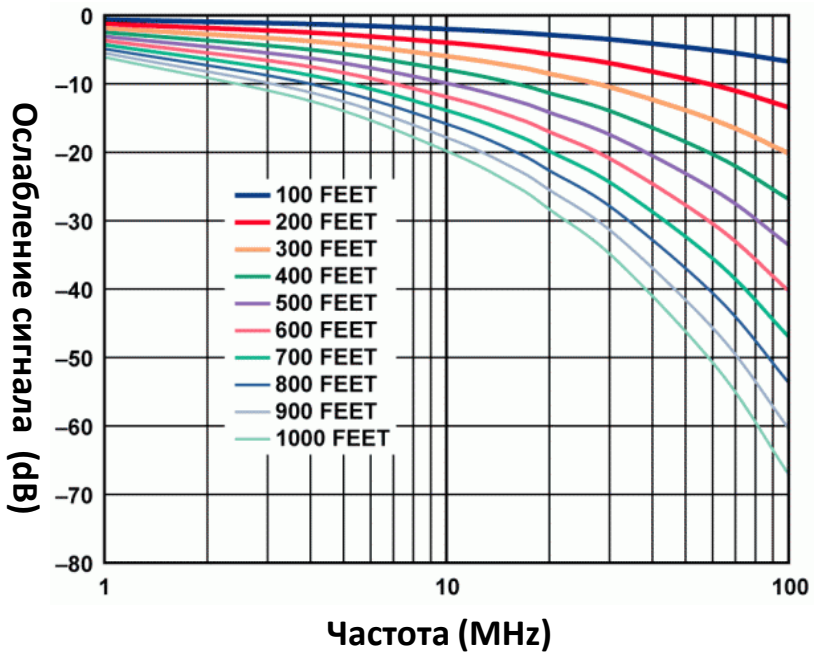
Причина межсимвольной интерференции

Эквивалентная модель длинной линии



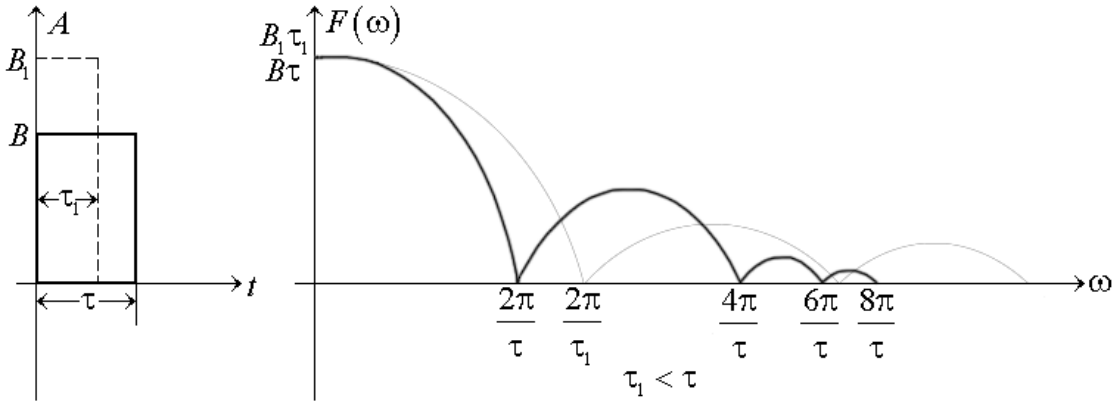
Из-за наличия сопротивления проводов, распределённой паразитной ёмкости и погонной индуктивности физическая линия по разному ослабляет сигналы разной частоты.

Причём, чем длиннее линия, тем больше ослабление верхних частот.



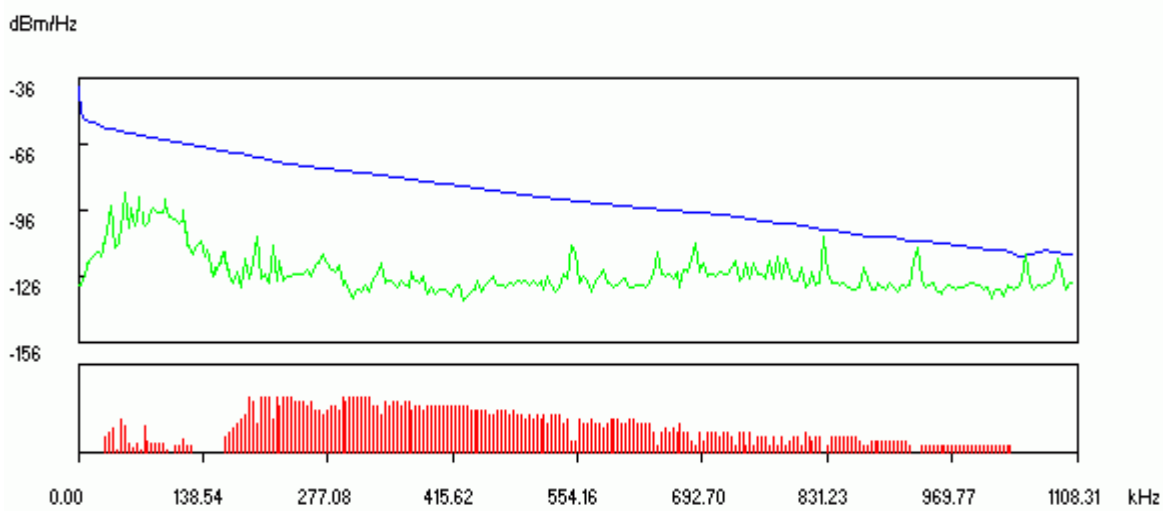
Спектр прямоугольного импульса

Чем короче импульс, тем более широким является его изначальный спектр и, следовательно, тем сильнее он будет искажаться в длинной линии



Шум (помехи) в каналах связи

Шум более-менее равномерно распределён по всему спектру, тогда как уровень полезного сигнала падает с возрастанием частоты.



В итоге начиная с некоторой частоты уровень шума становится больше уровня полезного сигнала

Теорема Шеннона

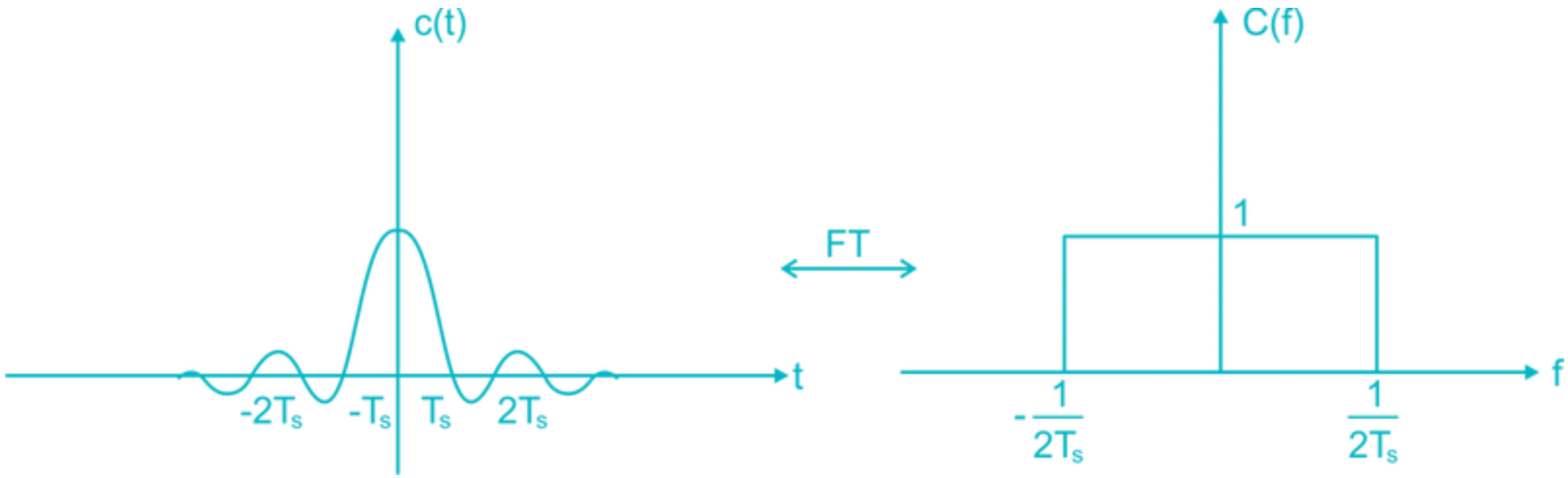
Теоретический наивысший предел скорости безошибочной передачи информации по аналоговому каналу с аддитивным Гауссовым шумом определяется как:

$$C = B * \log_2(1 + \frac{S}{N})$$

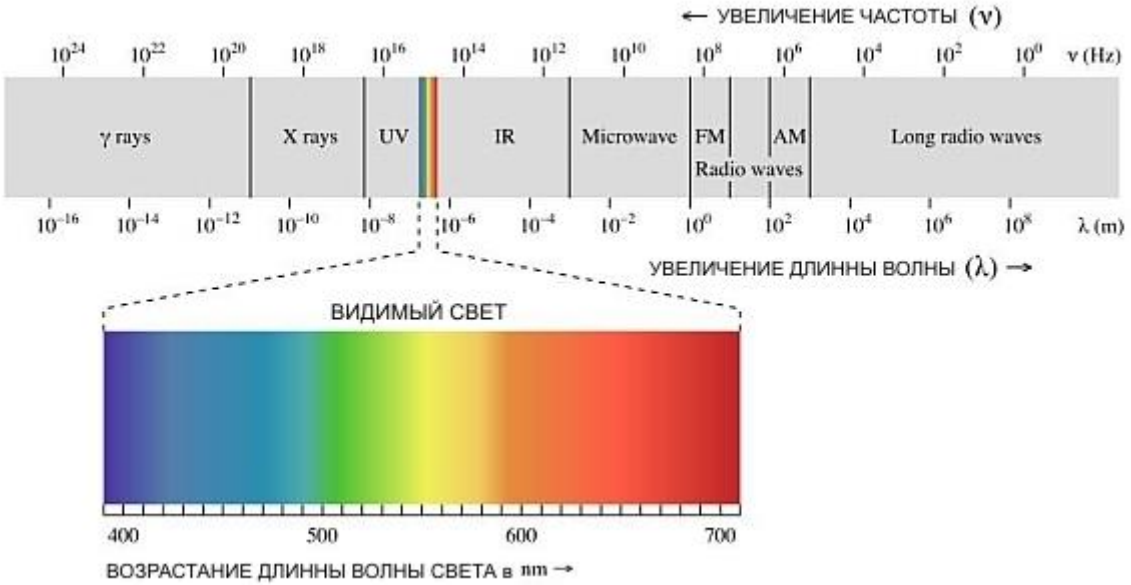
Где:

- C – верхний предел пропускной способности канала, *[бит/сек]*
- B – полоса пропускания канала, *[Гц]*
- S – полная мощность сигнала по всей полосе пропускания, *[Вт]*
- N – полная мощность шума по всей полосе пропускания, *[Вт]*

Импульс с прямоугольным спектром



Спектр электромагнитных излучений



План курса

1. Введение в компьютерные сети
2. Основные методы построения СПД
3. Архитектура Internet Protocol Suite (TCP/IP)
4. Архитектура модулей физического уровня
5. **Технологии беспроводных сетей**
6. Архитектура модулей канального уровня
7. Протоколы транспортного уровня
8. Технологии WWW

Классификация беспроводных сетей

WPAN (Wireless Personal Area Network) – беспроводные персональные сети, функционирующие на коротких расстояниях (как правило в пределах досягаемости отдельного человека): Bluetooth (IEEE 802.15.1), ZigBee (IEEE 802.15.4)

WLAN (Wireless Local Area Network) – беспроводные локальные сети, покрывающие отдельные помещения или аналогичные открытые площадки: WiFi (IEEE 802.11)

WMAN (Wireless Metropolitan Area Network) – беспроводные сети масштаба города/района: WiMAX (IEEE 802.16)

WWAN (Wireless Wide Area Network) – беспроводные глобальные сети, функционирующие, как правило, в сотовых сетях мобильной связи: GSM (GPRS, EDGE), 3G/UMTS (HSPA, HSPA+), LTE

Технологии «радио Ethernet» Wi-Fi

Wi-Fi – это *торговая марка* **Wi-Fi Alliance**, относящаяся к оборудованию для создания беспроводных сетей, соответствующих семейству стандартов IEEE 802.11

Стан-дарт	Диапа-зон (ГГц)	Полоса (МГц)	Моду-ляция	Скорость (Мбит/сек)	Примерная дальность (м)	MIMO
802.11b	2.4	22	DSSS	1, 2, 5.5, 11	35/140	-
802.11g	2.4	20	OFDM	6, 9, 12, 18, 24, 36, 48, 54	38/140	-
802.11n	2.4, 5	20	OFDM	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2	70/250	до 4
		40	OFDM	15, 30, 45, 60, 90, 120, 135, 150		

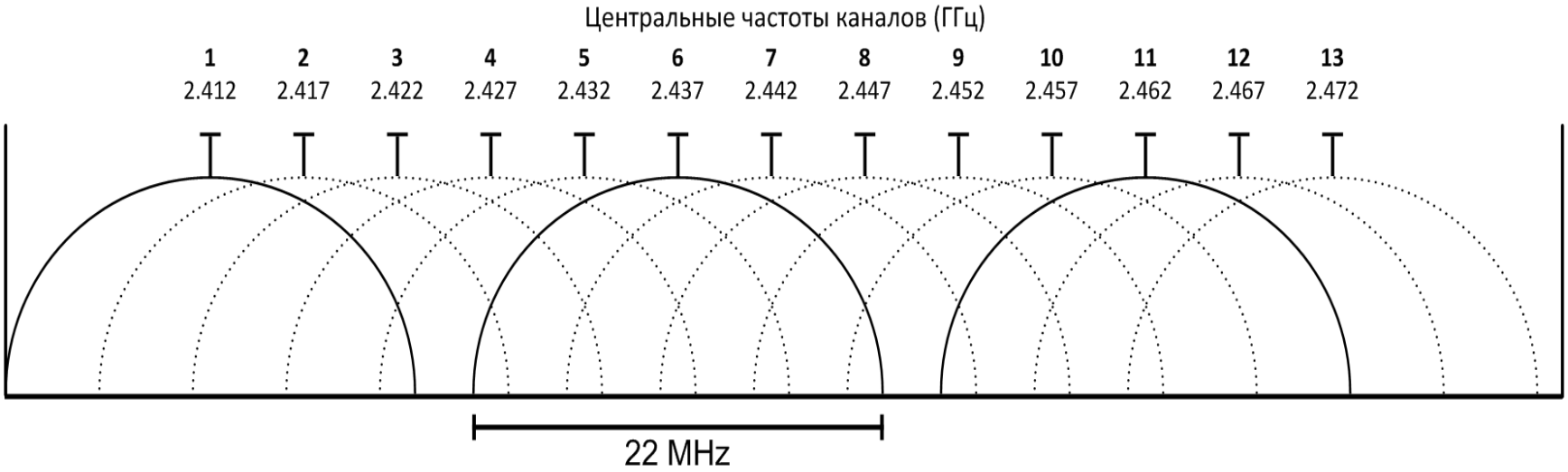
Используемые диапазоны:

2.4 ГГц (2,400–2,483.5 МГц) – дециметровые волны

5 ГГц (5,150-5,725 МГц) – сантиметровые волны

Диапазон 2,4 ГГц

В диапазоне 2,400-2,485 ГГц размещено 13 каналов шириной 22 МГц с перекрывающимся спектром:



Таким образом, не мешая друг другу могут одновременно работать только 3 станции (каналы 1, 6 и 11)

Данный диапазон (ISM – industrial, scientific, medical) используется также различным оборудованием, например, микроволновыми печами, которые создают помехи работе оборудования Wi-Fi

Структура и режимы работы сети Wi-Fi

Компоненты сети:

STA (station) – сетевая станция

AP (access point) – точка доступа

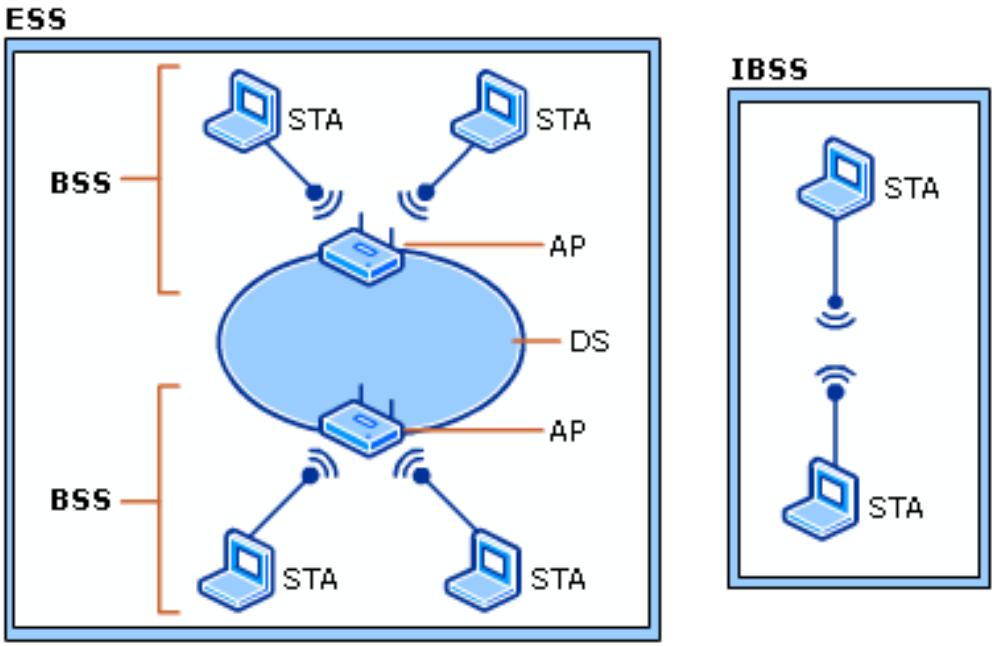
DS (distribution system) – сеть, посредством которой AP могут обмениваться пакетами

Режимы работы:

BSS (basic service set) или Infrastructure mode: одна AP и одна или несколько STA

IBSS (independent basic service set) или Ad-Hoc mode: две или более STA

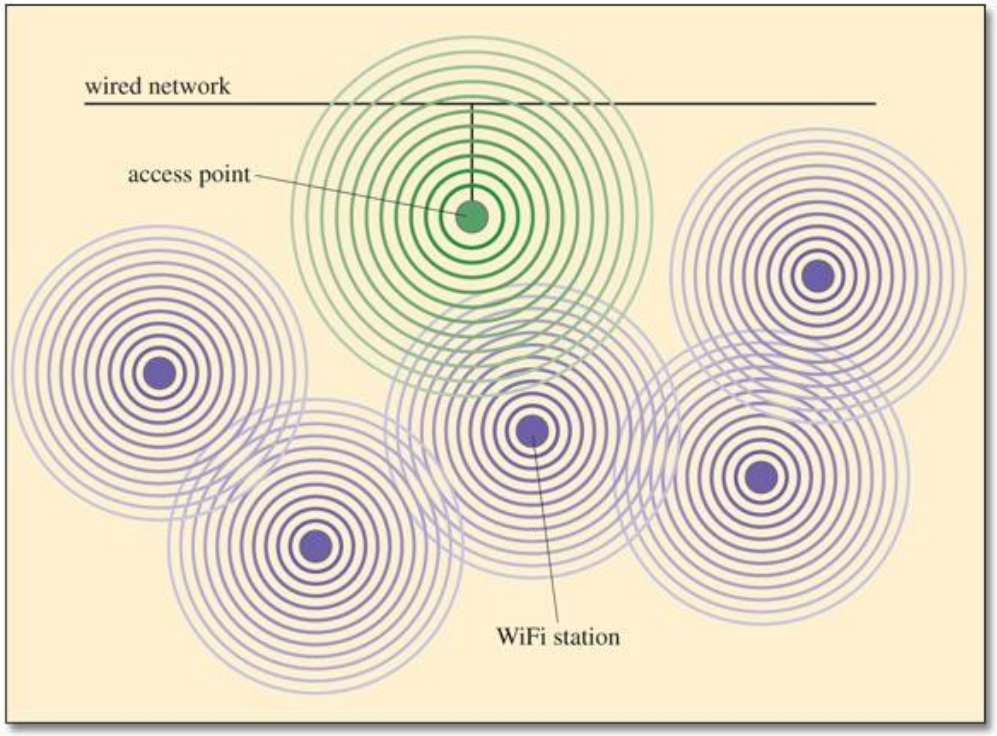
ESS (extended service set): несколько AP и несколько STA с возможностью roaming



AP, как правило, имеет возможность подключения к проводной сети Ethernet. При этом, обслуживаемые STA могут прозрачно обмениваться данными как между собой (через AP!), так и с проводными станциями

Физический принцип работы Wi-Fi

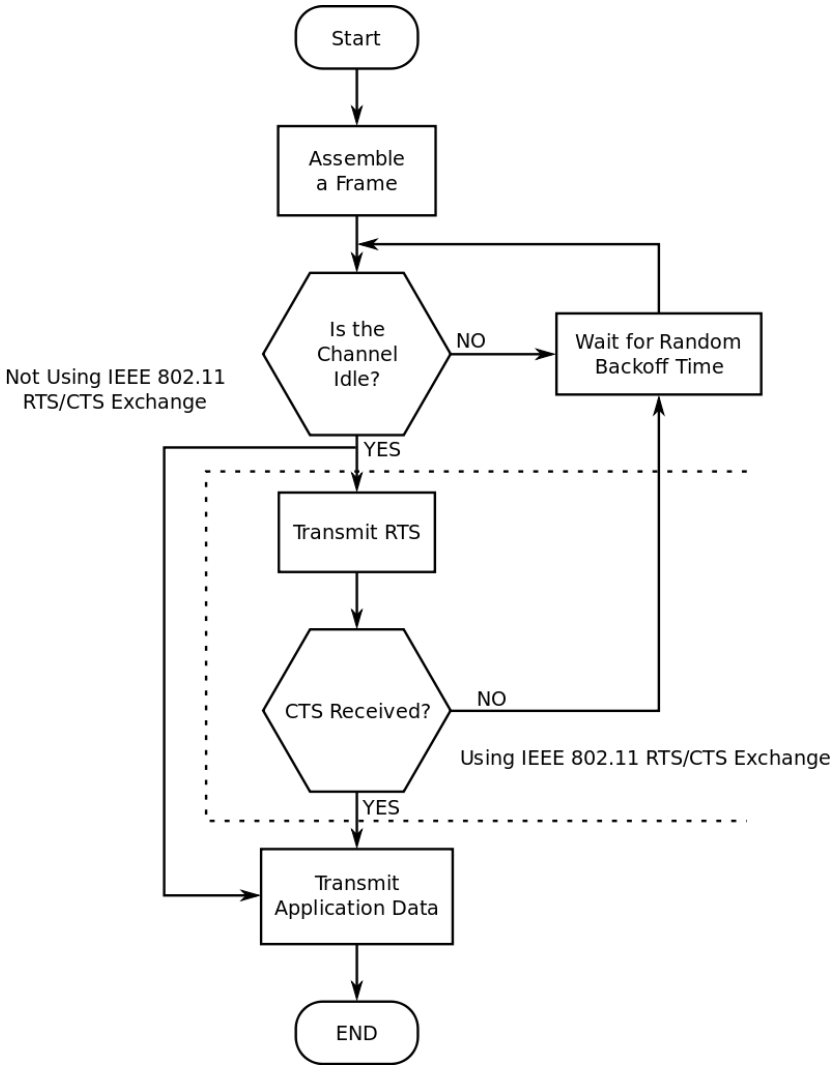
Все станции в беспроводном сегменте разделяют одну общую полудуплексную среду передачи в режиме соперничества.



Для минимизации коллизий используется метод **CSMA/CA** (Carrier Sense Multiple Access with Collision Avoidance)

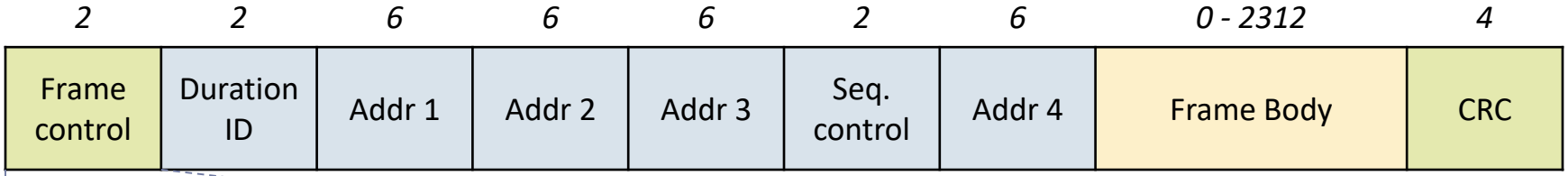
Принцип работы CSMA/CA

- ✓ Перед началом передачи проверить доступность среды (carrier sense)
- ✓ Если среда занята, то ожидать случайный интервал времени и снова проверить доступность среды
- ✓ Если среда свободна, то имеется два варианта поведения (в зависимости от размера передаваемого кадра, возможностей и настроек передающей станции):
  - ➢ Отправить кадр сразу
  - ➢ Использовать механизм RTS/CTS
- ✓ В последнем случае STA начинает передачу только получив от AP кадр CTS (clear to send) в ответ на RTS (request to send)

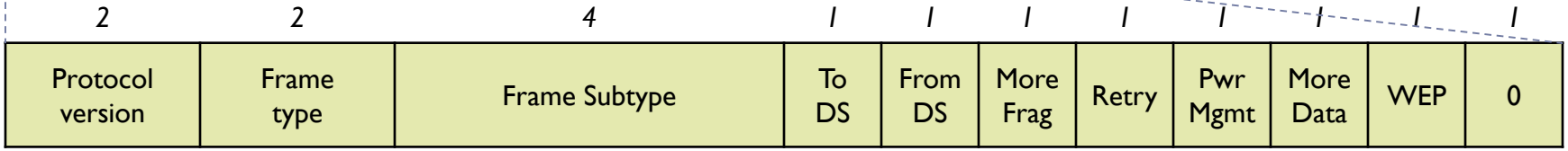


Структура передаваемого кадра

Байты:



Биты:



Frame type (тип кадра):

- **00** – Management
- **01** – Control
- **10** – Data

To DS – кадр следует в DS

From DS – кадр пришел из DS

More Frag – не последний фрагмент кадра

Retry – повторная передача

Duration ID – время в μs, необходимое для завершения передачи (в RTS/CTS)

Seq. control – номер кадра (12 бит) + номер фрагмента (4 бита)

Кадры управления и процедуры

Процедура	Наименование кадра	Пояснение
Аутентификация AP в сегменте	Authentication	Кадр протокола аутентификации
	Deauthentication	Logoff для AP
Ассоциация STA на AP	Association request	Запрос на подключение
	Association response	Ответ на подключение
	Reassociation request	Запрос повторного подключения
	Reassociation response	Ответ повторного подключения
	Disassociation	Отключение
Анонсирование AP	Beacon	Кадр-маяк

Кадр маяка AP

Кадр Beacon отправляется AP периодически для того, чтобы оповестить окрестные STA о своем существовании. Он содержит:

- Текущее астрономическое время AP;
- Интервал оповещения (отправки Beacon);
- Описание возможностей AP и подсети (capabilities);
- **SSID** (Service Set ID) – текстовое название Wi-Fi «сети» – до 32 байт;
- Параметры используемых способов модуляции
- и др.

Отправку SSID можно отключить (так устроены т.н. hidden AP).

Безопасность передаваемых данных

- Любая станция принципиально способна «слышать» кадры, передаваемые в эфире и может без особого труда «подслушивать» любой трафик без необходимости какой-либо регистрации или физического подключения.
- Если средства защиты не используются (точка доступа без пароля), то сетевой трафик по эфиру передается в открытом виде и тогда злоумышленник способен видеть все, что передается и даже более.
- Поскольку предотвратить «подслушивание» нельзя, Wi-Fi использует метод шифрования передаваемых данных. Однако шифроваться могут только данные кадра – все заголовки передаются в открытом виде (например, MAC адреса)
- В настоящее время доступно несколько вариантов шифрования:
  - WEP
  - WPA
  - WPA2-PSK
  - WPA2-Enterprise

Алгоритм защиты WEP

WEP (wire equivalent privacy) – конфиденциальность, эквивалентная проводной сети. Исторически первый метод, описанный в варианте стандарта IEEE 802.11-1998. На сегодняшний день не может считаться сколь-либо надежным и **легко взламывается** за время, измеряемое минутами !
Метод содержит несколько принципиальных уязвимостей, позволяющих вычислять значение секретного ключа шифрования путем сбора статистики кадров и отправки специальных пробных кадров.

Алгоритмы защиты WPA2

Wi-Fi Protected Setup (WPS)

Отключите WPS, если сможете.