Основы теории wi-fi

Еремеев Вади
Новые Системы Телеком
www.nstel.ru

Стандарты WLAN

IEEE 802.11 - самый первый стандарт WLAN, 1997 г, 1 Mbps и 2 Mbps, 2.4 GHz RF. В настоящее время часть 802.11b

IEEE 802.11a - стандарт 1999 г, 54 Mbps, 5 GHz RF

IEEE 802.11b - расширение 802.11, 5.5 and 11 Mbps (1999), 2.4 GHz

IEEE 802.11e - расширение для использования средств мультимедиа (2005)

IEEE 802.11F - Inter-Access Point Protocol (2003), описывает процедуру аутентификации при перемещении клиента между точками доступа

IEEE 802.11g - стандарт 2003 г, 54 Mbit/s, 2.4 GHz (обратно совместим с b)

IEEE 802.11i - расширение для использования шифрования WPA2 (2004)

IEEE 802.11n - стандарт 2008 г, увеличение скорости передачи до 600 Mbps, 2.4 & 5 Ghz RF

IEEE 802.11s - расширение для использования технологии Mesh

IEEE 802.11k - bandsteering (2.4 и 5 GHz)

IEEE 802.11r - fast roaming

IEEE 802.11u - (Hotspot 2.0) интеграция Wi-Fi с сетями других стандартов

IEEE 802.11ac - скорость передачи данных — до 6,77 Gbps (MIMO 8x8). Утвержден в январе 2014 года.

IEEE 802.11ad - стандарт с дополнительным диапазоном 60 ГГц (частота не требует лицензирования). Скорость передачи данных — до 7 Гбит/с.

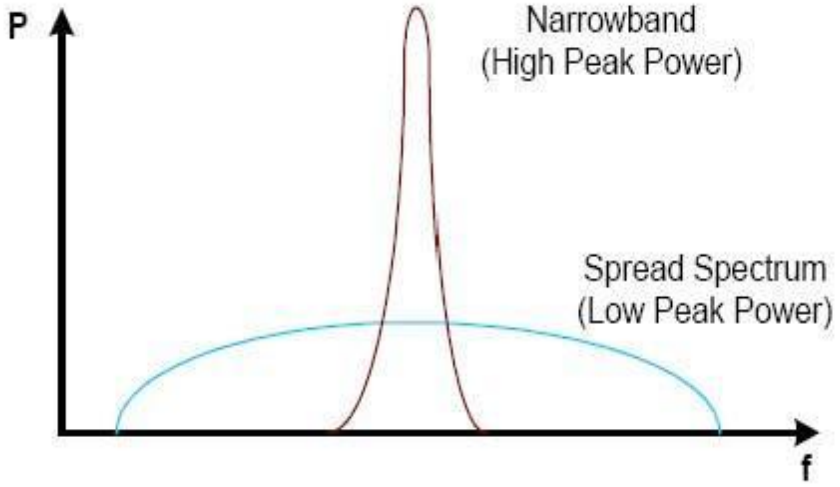
Узкополосные системы передачи и системы с расширенным спектром

Узкополосные системы:

- Используется минимальная полоса для передачи сигнала
- Узкая полоса, высокая мощность передачи сигнала
- Подвержены интерференции

Расширенный спектр:

- Используемая полоса много больше, чем необходимо для передачи информации
- Широкая полоса – низкая мощность передачи сигнала
- При интерференции теряется только небольшая часть информации, которая может быть передана повторно



Технологии распределённого спектра (Spread spectrum)

Метод частотных скачков (FHSS):

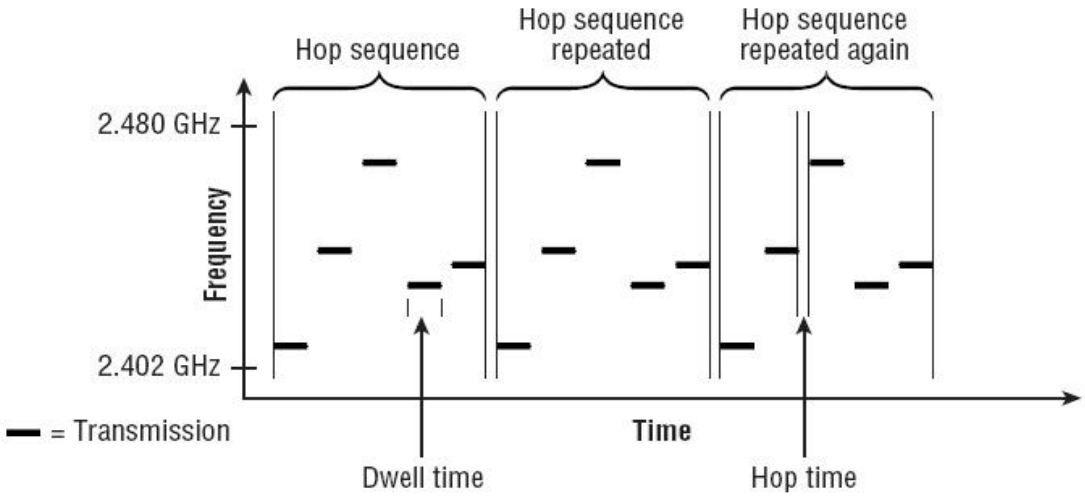
– Используется в 802.11

– Ограниченная пропускная способность (<2 Мбит/с)

– Одна информационная несущая

– Устойчивость к многолучевой интерференции

– В наст. время используется в Bluetooth (802.15)



Технологии распределённого спектра

Метод прямой последовательности (DSSS):

– Высокая пропускная способность

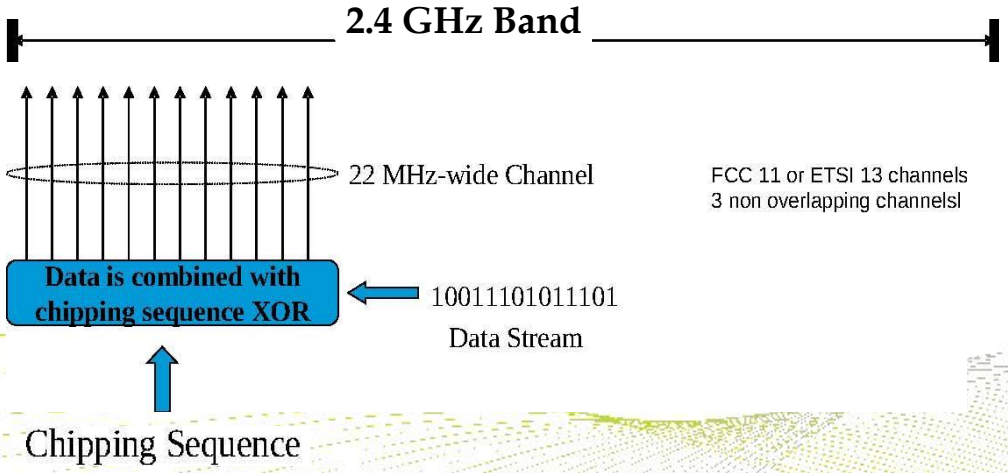
– Простота реализации

– Более высокая скорость кодирующей последовательности обеспечивает устойчивость к интерференции

– Реализуются различные методы модуляции несущих

– Множество информационных несущих

– В настоящее время используется в 802.11 WLAN



Технологии распределённого спектра

DSSS использует 11 битное избыточное кодирование Кодом Баркера. Каждый бит информации кодируется 11-ю битами кода. DSSS используется в 802.11, получаемые скорости 1 и 2 Мбит/с.

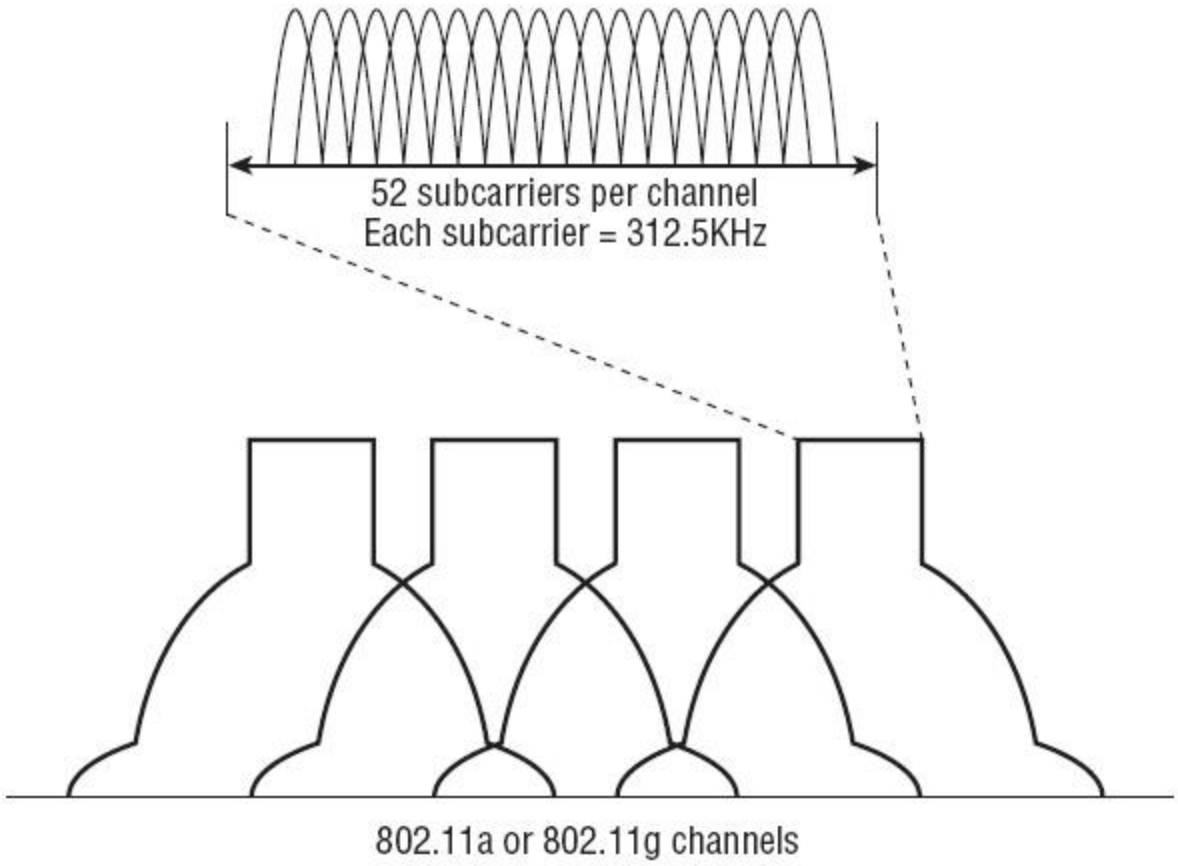
HR-DSSS (высокоскоростная DSSS технология) использует 8-ми битное избыточное кодирование CCK (Complementary Code Keying). CCK используется в 802.11b. CCK позволяет кодировать 4 бита данных 8-ми битным кодом – 5.5 Мбит/с, 8 бит данных 8-ми битным кодом – 11 Мбит/с.

Технология OFDM

Orthogonal Frequency Division Multiplexing (ортогональное частотное мультиплексирование) – технология, используемая в 802.11a стандарте, позволяет передавать данные до 54 Мбит/с. OFDM не является технологией расширенного спектра, но обладает похожими свойствами: низкая мощность передачи, использование более широкой полосы, чем требуется для передачи данных. OFDM использует 52 субчастоты, 48 используется для передачи данных, 4 – служебные.

ERP-OFDM – Extended Rate Physical OFDM – расширение OFDM для диапазона 2.4 ГГц. Используется в 802.11g стандарте, также позволяет передавать данные до 54 Мбит/с.

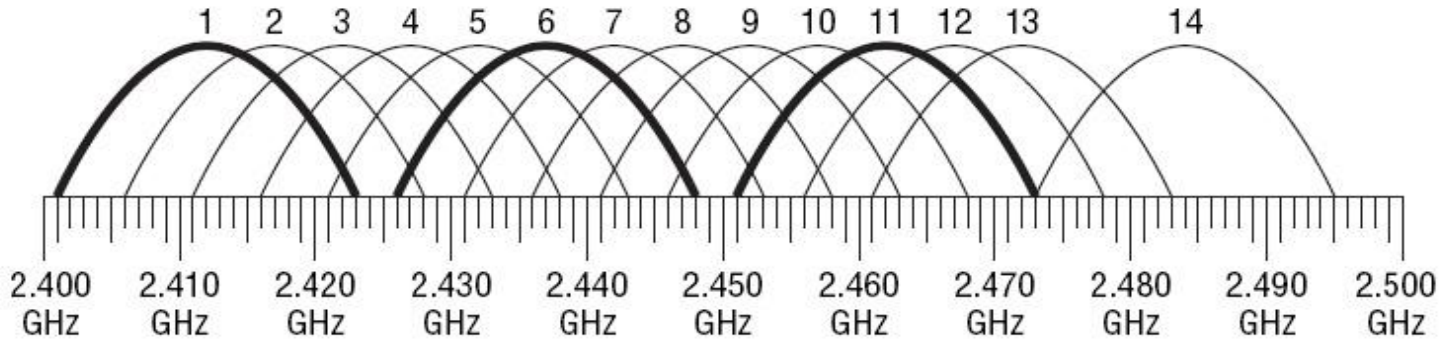
Технология OFDM



Модуляция

IEEE стандарт	Технология кодирования/ модуляция	WLAN скорость
802.11	Barker Code/DBPSK, DQPSK	1 and 2 Mbps
802.11 b	Complementary Code Keying (CCK)/DQPSK	5.5 and 11 Mbps
802.11g/a	OFDM (Orthogonal frequency-division multiplexing)/ BPSK, 4-QAM, 16-QAM, and 64-QAM	6, 9, 12, 18, 23, 36, 48 and 54 Mbps

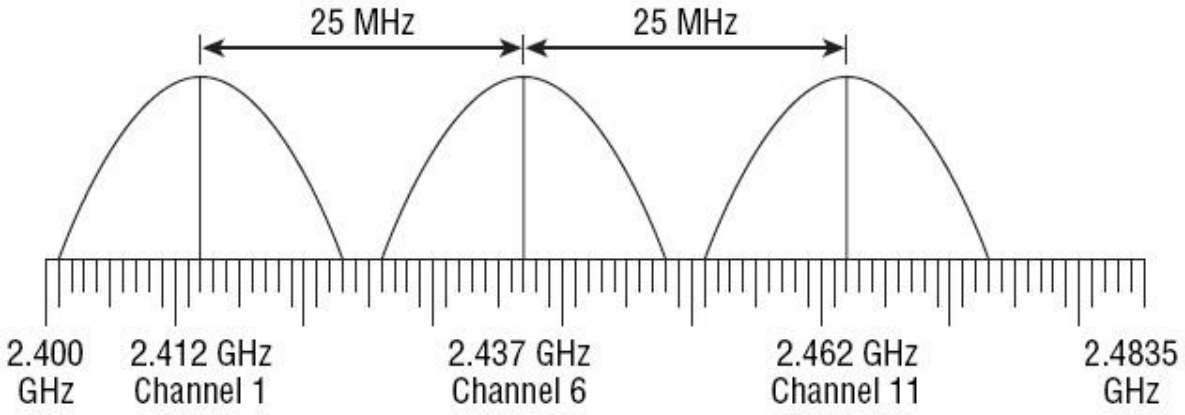
DSSS каналы



№ ch	1	2	3	4	5	6	7	8	9
F, GHz	2,412	2,417	2,422	2,427	2,432	2,437	2,442	2,447	2,452
№ ch	10	11	12	13	14				
F, GHz	2,457	2,462	2,467	2,472	2,484				

DSSS каналы

По стандарту между несущими должен быть разнос не менее 25 МГц, т.о. в 802.11 b/g может быть 3 непересекающихся канала – обычно 1, 6, 11.



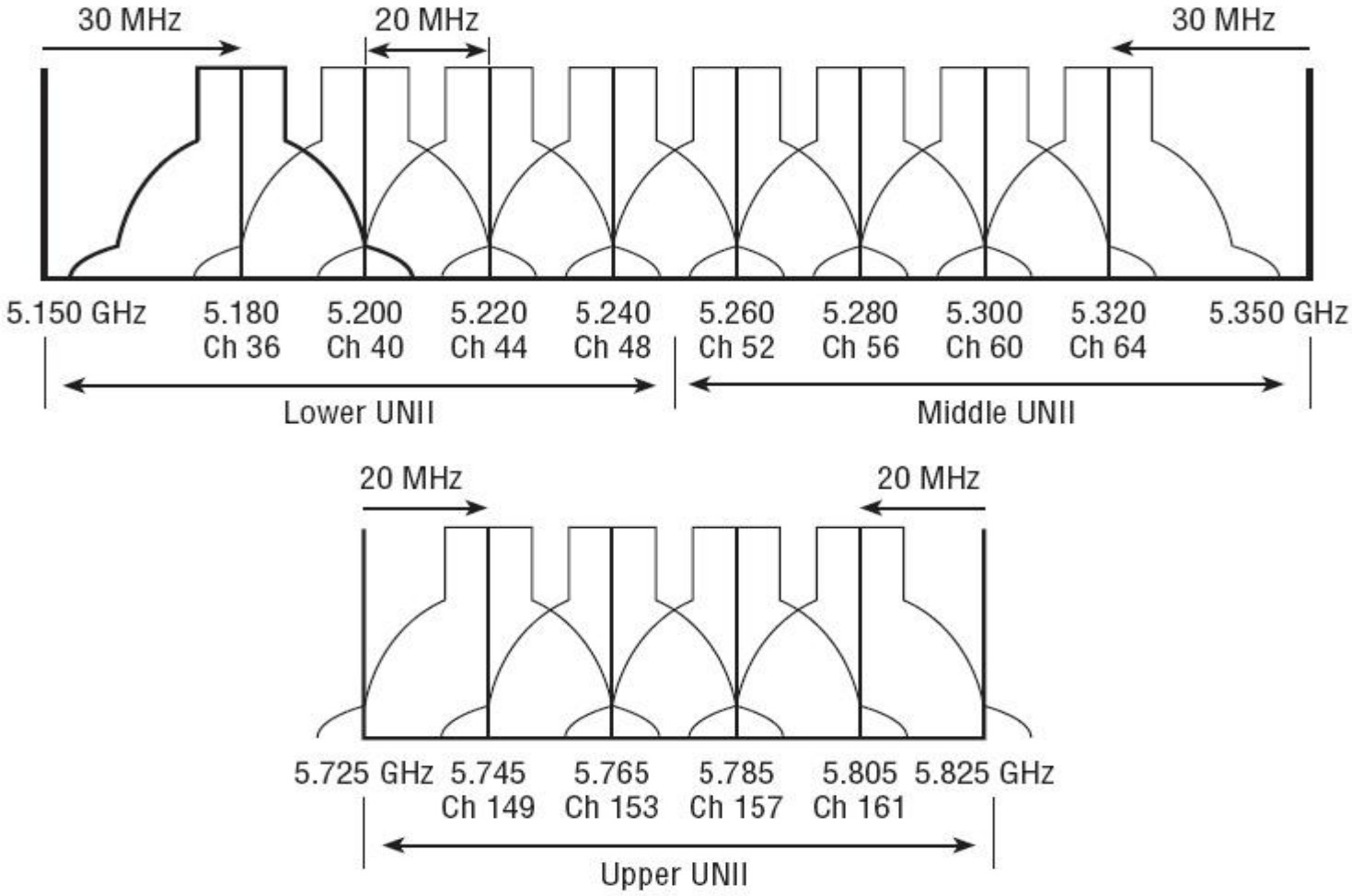
Число каналов, разрешённые различными организациями:

FCC 11 каналов

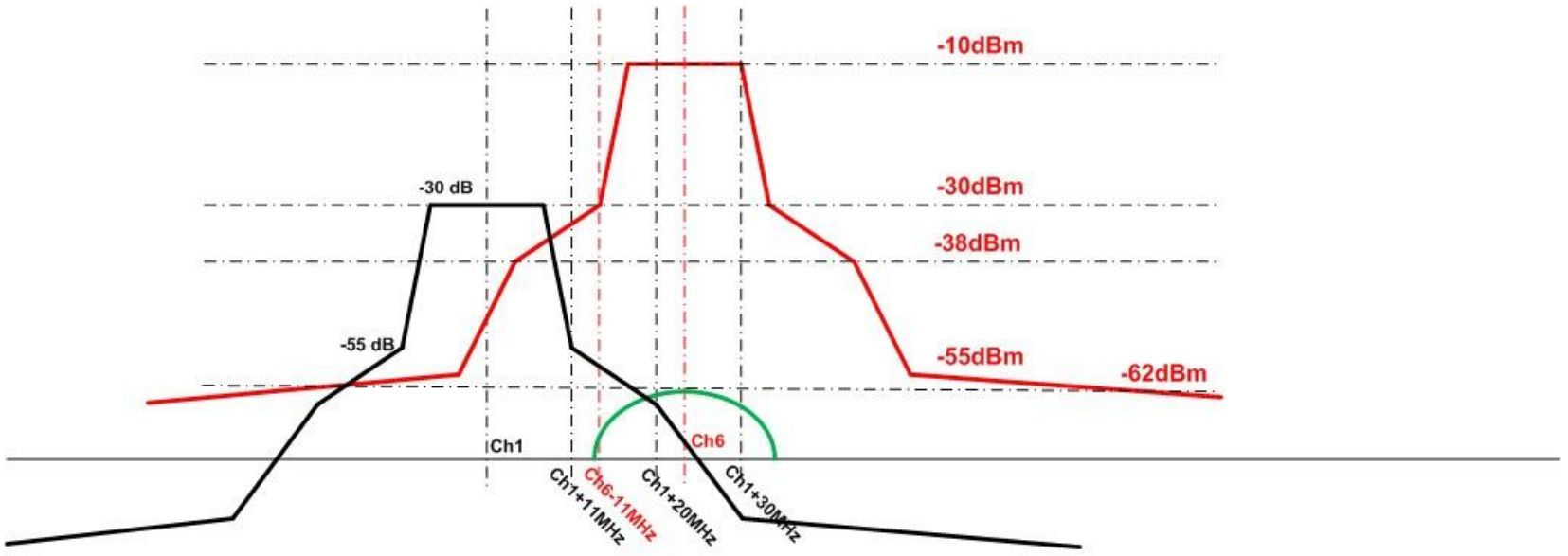
ETSI 13 каналов

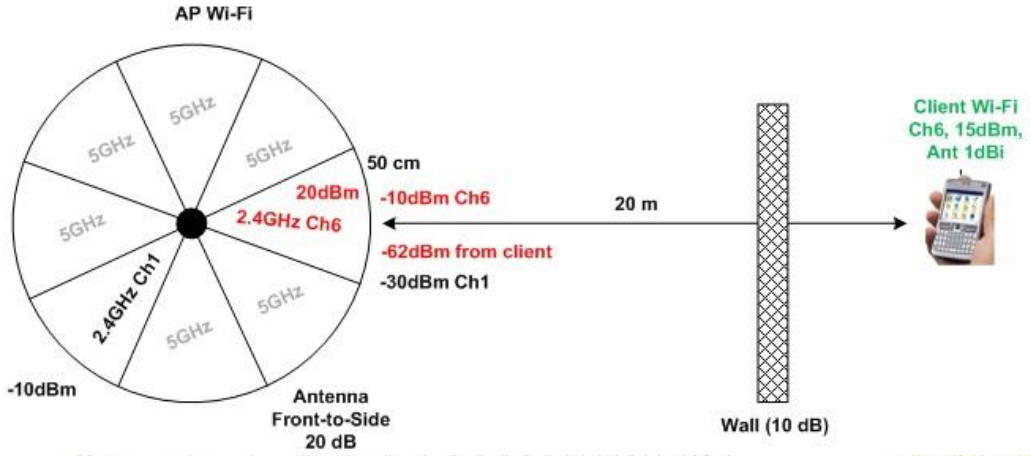
Japan 14 каналов

OFDM каналы


30 MHz
20 MHz
30 MHz
5.150 GHz
5.180
Ch 36
5.200
Ch 40
5.220
Ch 44
5.240
Ch 48
5.260
Ch 52
5.280
Ch 56
5.300
Ch 60
5.320
Ch 64
5.350 GHz
Lower UNII
Middle UNII
20 MHz
20 MHz
5.725 GHz
5.745
Ch 149
5.765
Ch 153
5.785
Ch 157
5.805
Ch 161
5.825 GHz
Upper UNII

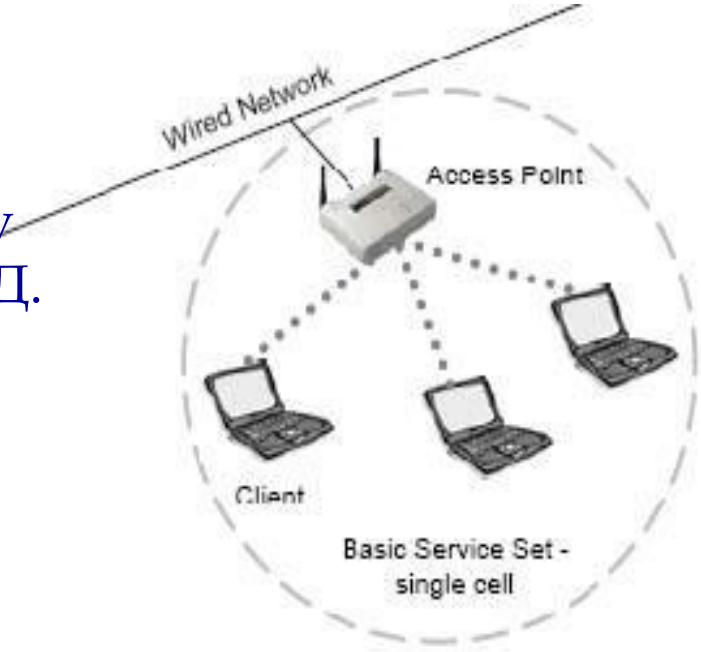
Взаимовлияние соседних каналов





Терминология WLAN

BSS – Basic Service Set (комплект базовой службы) – точка доступа и клиент/клиенты. Базовый означает только одна ТД/”одна сота”
BSS относится к “инфраструктурному режиму” --режим, который требует ТД.
Весь беспроводной трафик проходит через точку доступа. Прямой обмен клиент-клиент не допускается.
BSS имеет уникальный SSID

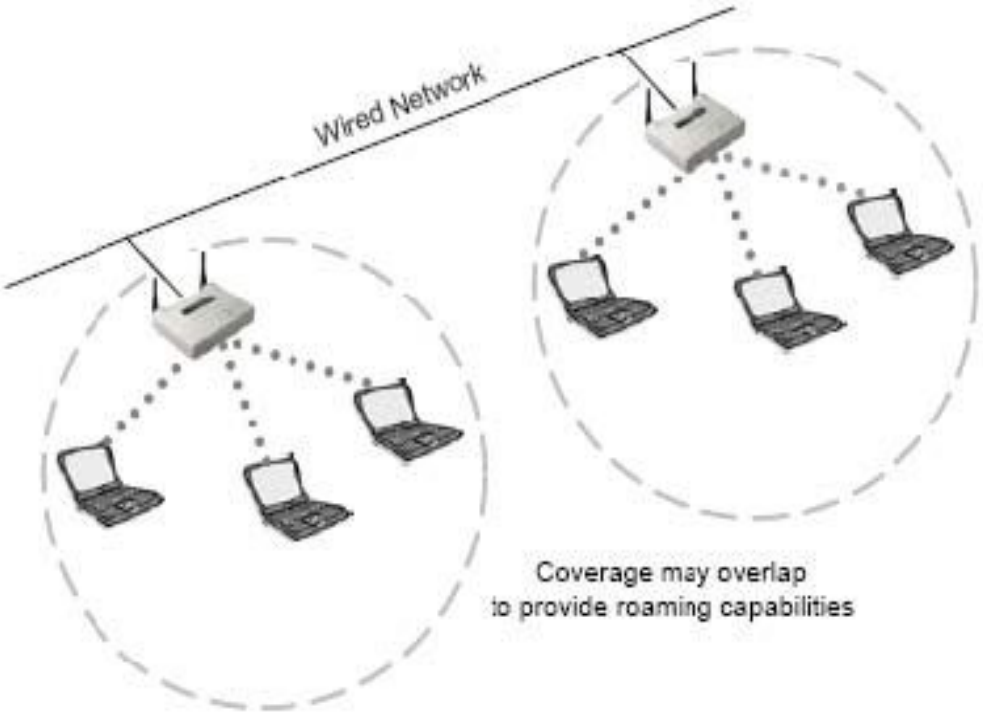


Терминология WLAN

SSID – чувствительное к регистру уникальное имя WLAN (от 2 до 32 символов)
SSID устанавливаются администратором на ТД (м.б. несколько SSID на ТД)
SSID включается во все пакеты на WLAN (в т.ч. в кадры beacon, probe request, probe response)
Только устройства с равными SSID могут обмениваться информацией
На клиентской станции необходимо указать с каким SSID (с какой WLAN) она будет работать

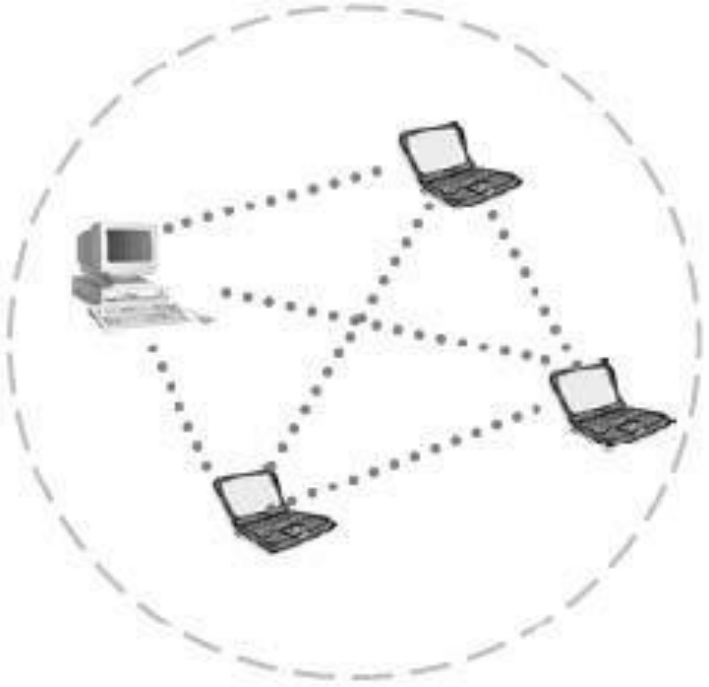
Терминология WLAN

ESS – комплект расширенной службы – определяет два или более BSS соединенных через распределительную сеть. Все пакеты в ESS должны проходить через одну из ТД.



Терминология WLAN

IBSS – независимый комплект базовой службы – не имеет ТД.
Покрывает одну ячейку и имеет один SSID.
IBSS известна как ad-hoc сеть (равный с равным).
Для передачи данных вне IBSS один из клиентов должен действовать как шлюз или маршрутизатор.



Терминология WLAN

Beacon – короткий кадр, который посылается из ТД к клиенту (в инфраструктурном режиме) или от клиента-к-клиенту (в ad-hoc режиме) для организации и синхронизации беспроводной связи.

Beacon обслуживает следующие функции:

– Синхронизация (станции корректируют свои часы, получают информацию о beacon интервале);

– Параметры DSSS (информация о канале);

– Информация об SSID;

– TIM (Traffic Indication Map) (указывает для какого клиента есть пакеты в буфере ТД);

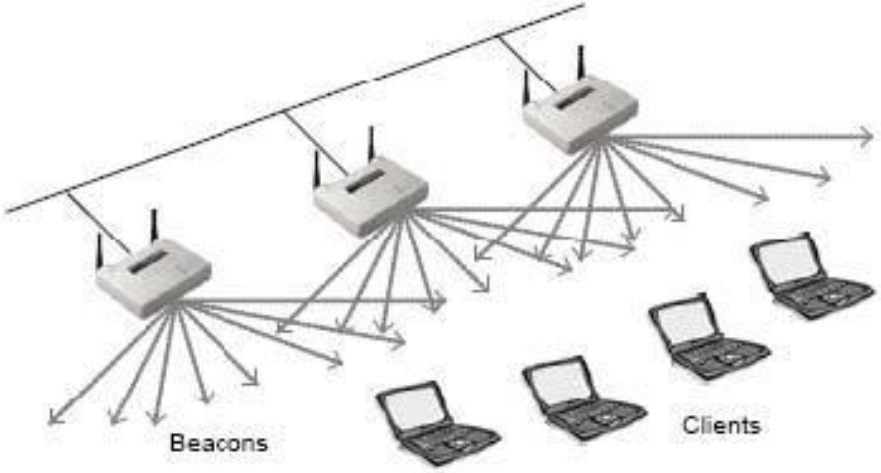
– Поддерживаемые скорости (информирует клиентов о поддерживаемых ТД скоростях).

Пассивное сканирование

ТД шлют beacons со след. информацией:
– SSID, канал, синхронизация, поддерживаемые скорости и др.
Клиенты пассивно сканируют радиоканалы для приема beacons.
Клиенты выбирают ТД с “правильным” SSID и пробуют ассоциироваться с ней.

Если несколько ТД используют один SSID, то выбирается соединение с наилучшими параметрами (сила сигнала, минимальные ошибки и т.п.).

Клиенты остаются в режиме сканирования (для обеспечения роуминга/ хэндовера к другой ТД).

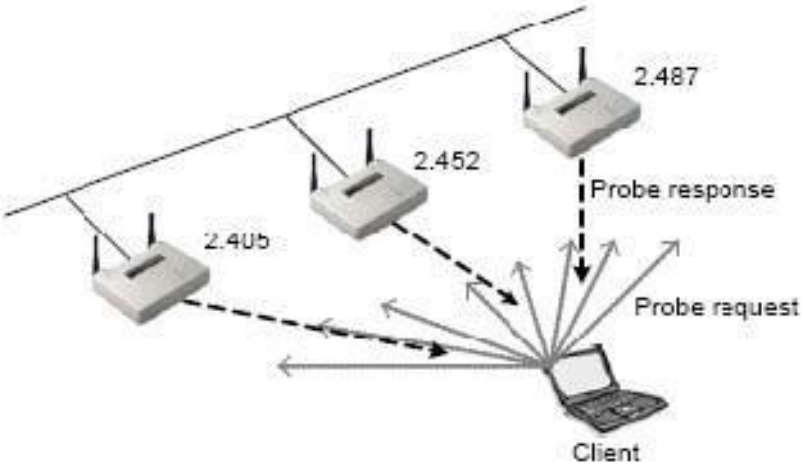


Активное сканирование

Станции шлют probe запрос со след. информацией:
– SSID, канал, поддерживаемые скорости и др;
– SSID м.б. Broadcast SSID.

Если указан конкретный SSID, то отвечает ТД с этим SSID, если указан broadcast SSID, то отвечать будут все станции в зоне досягаемости станции.

После определения ТД, через которую станция подключится к сети, начинается процесс аутентификации и ассоциации.



Аутентификация и ассоциация

Аутентификация (всегда предшествует ассоциации) – процесс проверки идентичности беспроводного узла (PC карты, USB адаптера, но не пользователя) сетью к которой узел пытается подключиться (т.е. что это тот узел за которого он себя выдает).

– Клиент посылает кадр аутентификационного запроса к ТД;

– ТД либо принимает, либо отвергает этот запрос, уведомляя клиента кадром аутентификационного ответа.

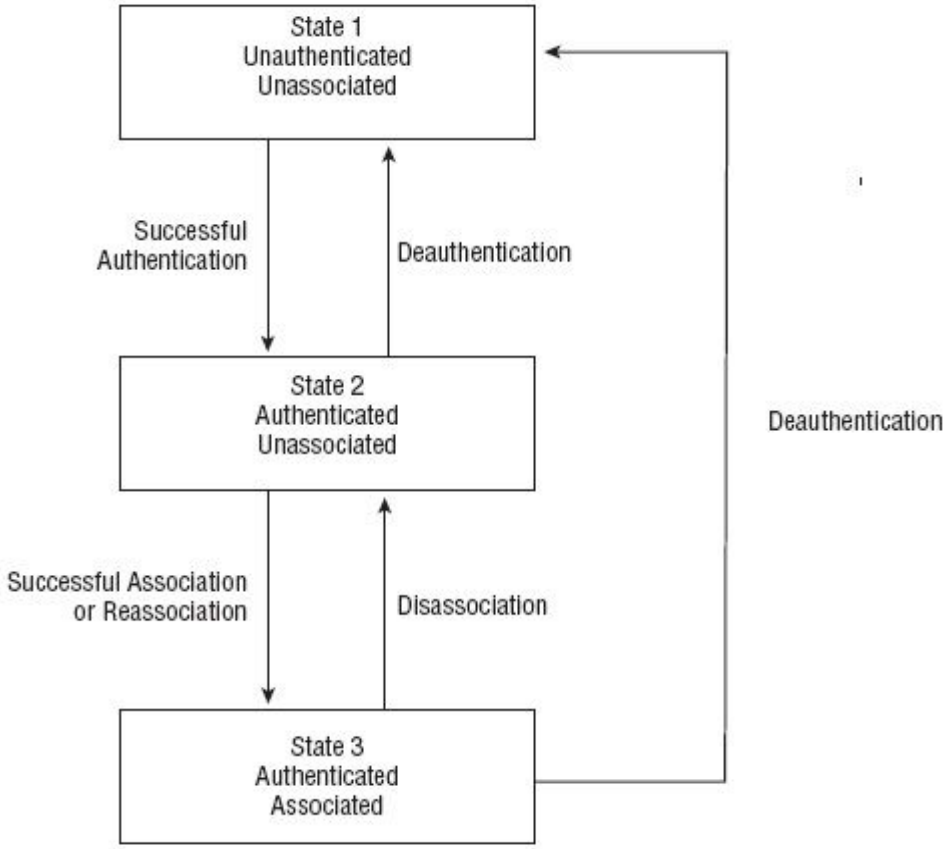
Процесс аутентификации может выполняться на ТД или ТД может передать это право далее вверх по потоку аутентификационному серверу (например, RADIUS).

Ассоциация – состояние в котором клиенту позволено передавать данные через ТД.

– После успешного завершения аутентификации станция посылает кадр запроса на ассоциацию (assotiation request);

– ТД отвечает кадром assotiation response позволяя или запрещая ассоциацию.

Аутентификация и ассоциация



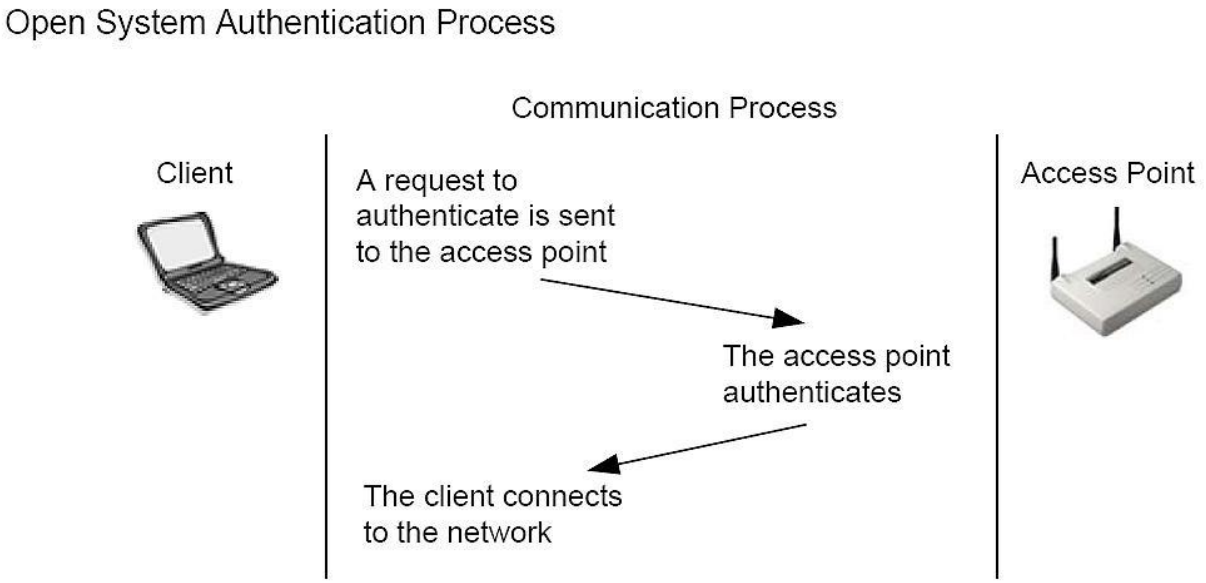
Методы аутентификации

Open system

- Только ассоциация на основе совпадения SSID
- WEP для шифрования трафика

Состоит из 4-х шагов:

1. клиент шлёт AUTH фрейм на ТД;
2. ТД отвечает клиенту ACK;
3. ТД шлёт клиенту AUTH фрейм с подтверждением аутентификации;
4. клиент отвечает ТД ACK.



Методы аутентификации

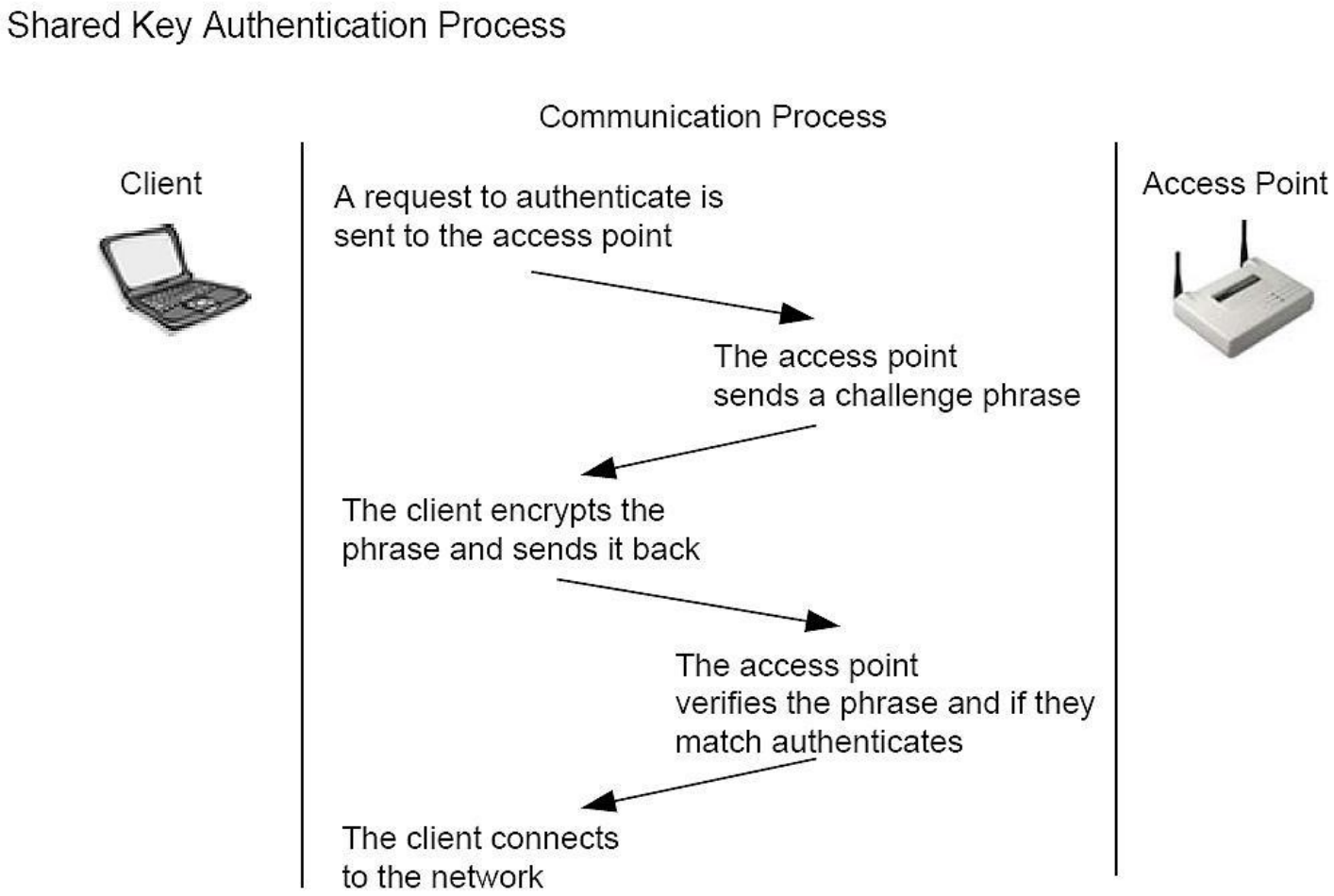
Shared Key

– Аутентификация на основе проверки ключей WEP;

– Более уязвимый и менее безопасный метод (по сравнению с Open System). Состоит из 8-ми шагов.

1. клиент шлёт на ТД AUTH фрейм с указанием использования Shared Key аутентификации;
2. ТД отвечает ACK;
3. ТД шлёт клиенту 2-й AUTH фрейм с содержанием 128 бит текста, который должен быть зашифрован;
4. клиент отвечает ACK;
5. клиент шифрует текст, используя статический WEP алгоритм и шлёт его на ТД в 3-м AUTH фрейме;
6. ТД отвечает ACK;
7. ТД расшифровывает текст и сравнивает с исходным. При совпадении результата клиенту отсылается 4-й AUTH фрейм, подтверждающий аутентификацию, при несовпадении – отвергающий;
8. клиент отвечает ACK.

Методы аутентификации



Методы аутентификации

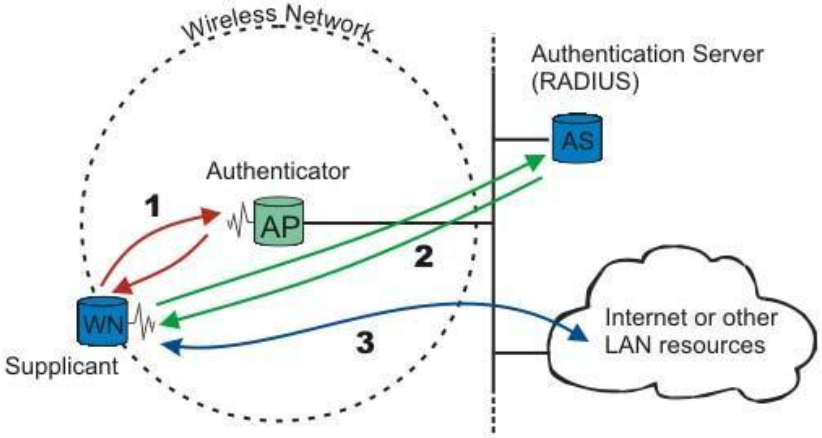
802.1x & EAP

– 802.1x – реализует схему взаимной аутентификации клиента и ТД. Схема использует сервер аутентификации и протокол аутентификации;

– EAP представляет и обрабатывает пользовательские мандаты (цифровой сертификат, имя-пароль, ID и т.п.). EAP-MD-5, LEAP, EAP-TLS, EAP-TTLS, EAP-SRP, EAP-SIM – различные реализации EAP.

WPA (Wi-Fi Protected Access)/WPA2 (802.11i) – метод защиты и целостности данных использующий управление ключами и новейшие математические методы шифрования

WPA(WPA2) -PSK – SOHO аутентификация



Категории WLAN фреймов

Management Frames

- Association request & response
- Reassociotion request & response
- Probe request & response
- Beacone
- ATIM
- Disassociation
- Authentification
- Deauthefication

Control Frames

- Request to sent (RTS)
- Clear to sent (CTS)
- Acknowledgement (ACK)
- Power-Save poll (PS poll)
- Contention-Free End (CF End)
- CF End + CF Ack

Data Frames

Обработка коллизий

Радиополоса WLAN – разделяемая среда
Невозможно определить наличие коллизий в WLAN, поэтому используется CSMA/CA (Collision Avoidance) вместо CSMA/ CD (в Ethernet)

CDMA/CA

– Передающая станция посылает пакет;

– Принимающая станция шлет обратно ACK, если она приняла пакет;

– Если посылающая станция не получает ACK, значит предполагается наличие коллизии и передача будет повторена;

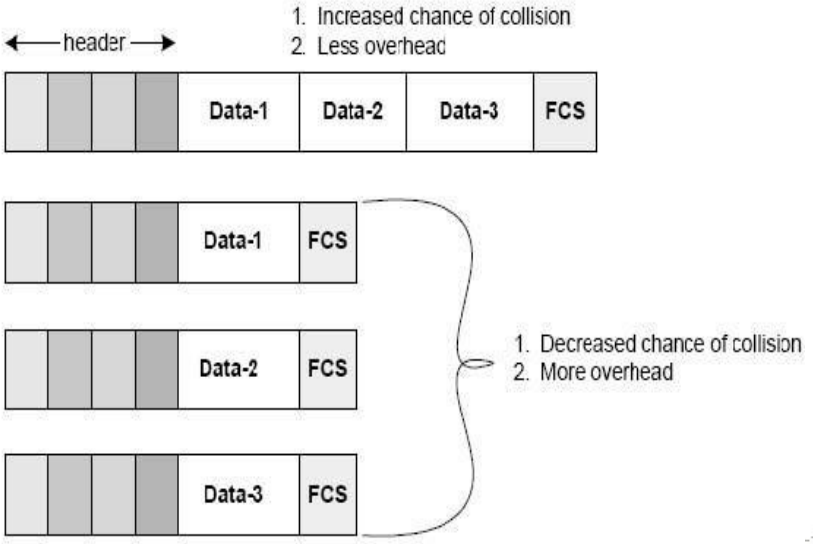
– Если физические или логические механизмы станции определяют занятость среды передачи, то после освобождения среды станция начнет передавать через случайный промежуток времени (random back off time).

Фрагментация

802.11 поддерживает фрагментацию

Не фрагментируются только широковещательные и групповые (multicast) пакеты.

Уменьшение порога фрагментации позволяет увеличить производительность если наблюдается большой уровень ошибок.

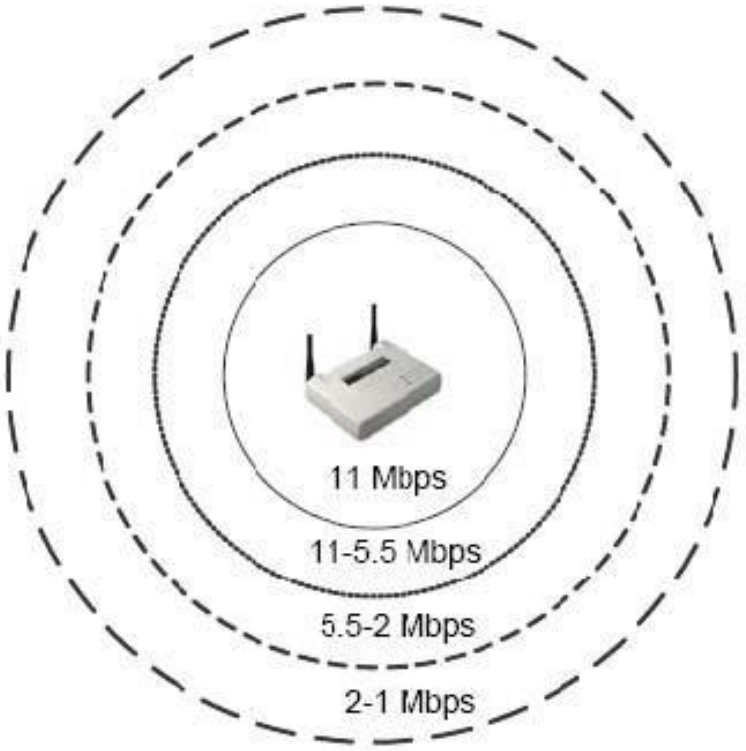


Dynamic Rate Shifting (DRS)

Dynamic Rate Shifting (DRS) или **Adaptive Rate Selection** (ARS) – метод динамического уменьшения скорости передачи на WLAN станции.

Изменение скорости происходит при ухудшении уровня принимаемого сигнала.

Скорость устанавливается к заданным дискретным значениям.



Coordination functions

Distributed Coordination Function (DCF) – метод конкурентного доступа к среде передачи (определенный в 802.11), использующий CSMA/CA.

Режим DCF используется во всех WLAN архитектурах (BSS, ESS, IBSS).

Point Coordination Function (PCF) – режим передачи, допускающий свободный от конкуренции доступ к среде передачи путем использования механизмов опроса (polling).

PCF дает возможность реализации механизмов QoS.

Не может быть применен в конфигурации ad-hoc.

DCF может использоваться без PCF. PCF – нет.

PCF создает большой избыточный трафик (overhead) и менее масштабируем, чем DCF.

Межкадровый промежуток

Interframe spacing (IFC) - используются для управления доступом к среде передачи

Три типа IFS

– SIFS – Short IFS (10 мксек) – время, после которого посылаются кадры: RTS, CTS, ACK. Обеспечивает максимальный приоритет доступа к среде передачи;

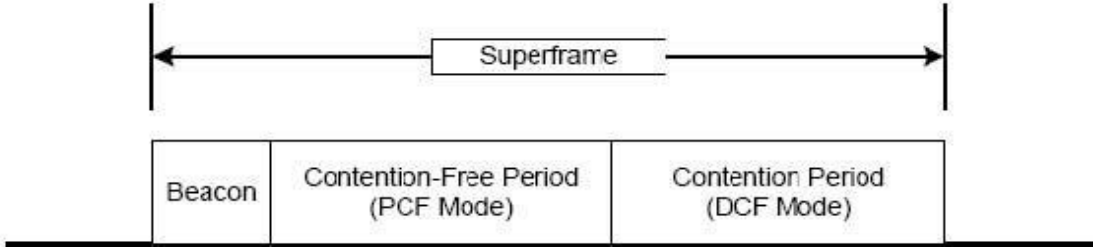
– PIFS – Point Coordination IFS (30 мксек) – используется в режиме PCF. Обеспечивает приоритет режима PCF перед DCF;

– DIFS – Distributed Coordination IFS (50 мксек) – время после которого станции в режиме DCF начинают “борьбу” за доступ к среде передачи (Contention Period).

Коммуникационные процессы

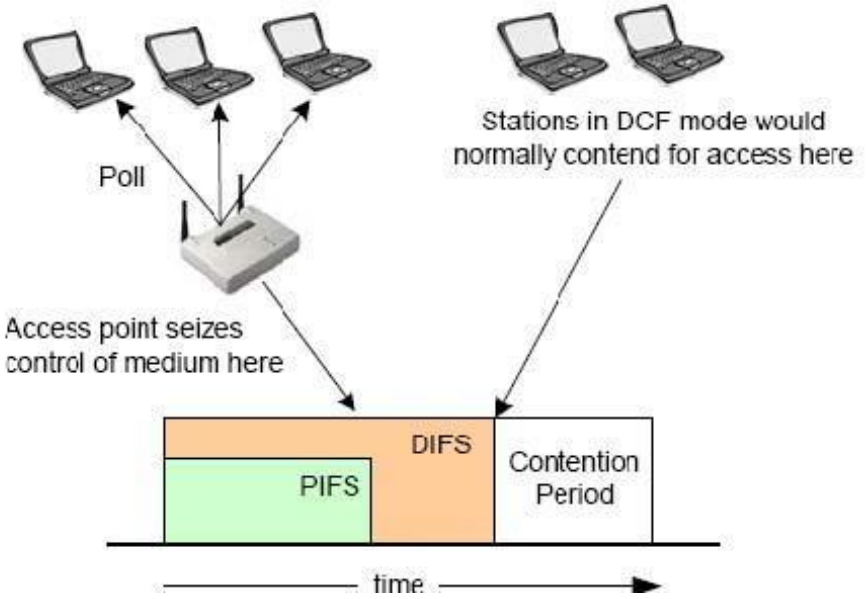
PCF и DCF

Точка доступа шлет beacon (broadcast)
В течение PCF ТД опрашивает станции на необходимость посылки данных
Если станция желает послать данные, она отправляет один кадр, если нет – возвращает null кадр для ТД
Опрос (polling) продолжается в течение Contention-Free периода
Затем станция переходит в DCF режим
Суперкадр заканчивается с концом CP (Contention Period)



Коммуникационные процессы

PCF и DCF

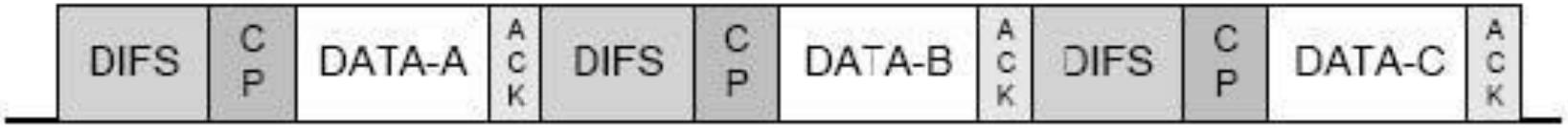


PIFS < DIFS, поэтому в CFP ТД захватывает среду передачи для опроса. После CFP ТД переключается в режим DCF.

Коммуникационные процессы

DCF

Станция ожидает, когда DIFS истечет;
В течение CP станция считает ее random back off (rand * slot time);
В конце каждого slot time периода проверяется занятость среды и станция с наименьшим временем первая получает контроль среды передачи;
Станция посылает данные;
Получающая станция ждет SIFS перед посылкой ACK станции, передающей данные;
Передающая станция получает ACK и процесс начинается сначала с новым DIFS.



RTS/CTS

Два механизма обнаружения занятости среды передачи:

– Физический на основе RSSI (Received Signal Strength Indicator);

– Логический, использующий Network Allocation Vector (NAV) и реализуется через RTS/CTS протокол (расширение CDMA/CA).

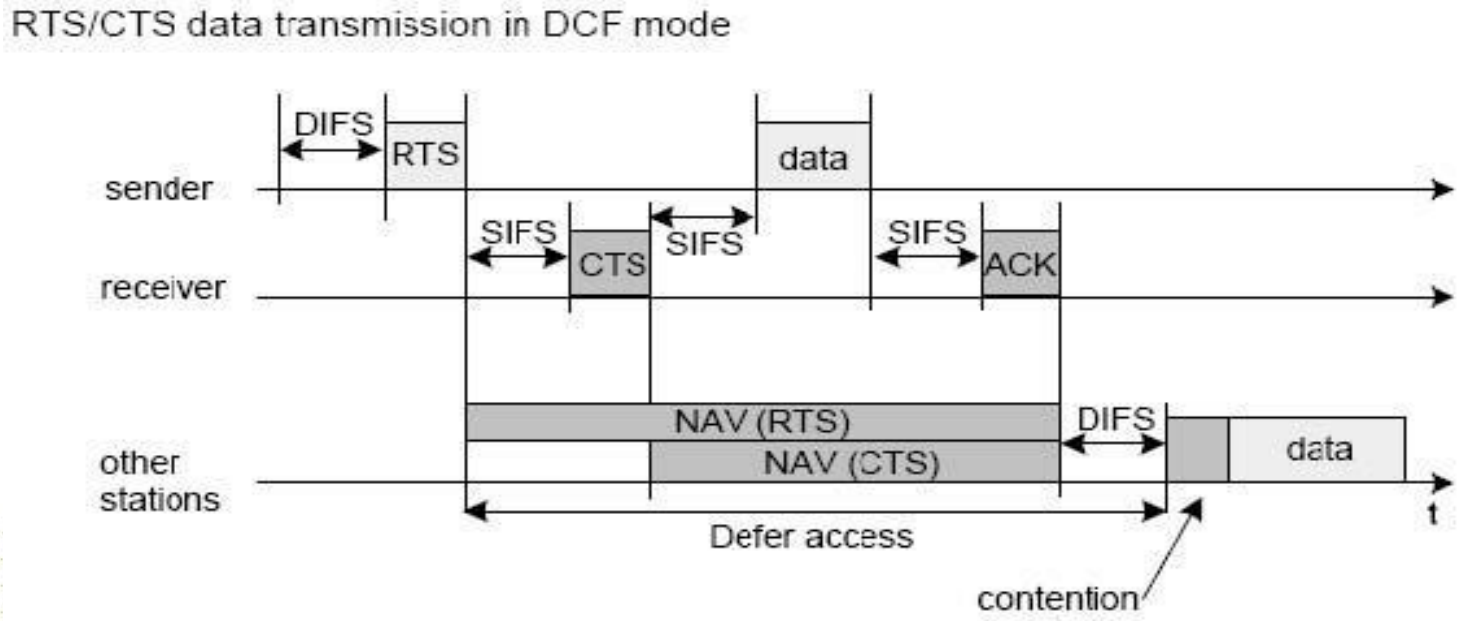
По умолчанию “OFF”. Целесообразно использовать при наличии большого количества коллизий в сети.

RTS/CTS

Кадр RTS – резервирует среду передачи для станции (установит поле NAV для всех станций, слышавших этот кадр на время необходимое для завершения передачи плюс возвращение ACK).

Кадр CTS – ответ на RTS, чтобы гарантировать, что все остановят передачу.

ACK – используется для уведомления посылающей станции, что данные прибыли в читаемом формате на принимающую станцию.



Модуляция

	Spreading Code	Modulation Technology	Data Rate
2.4 GHz DSSS	Barker Code	DBPSK	1 Mbps
	Barker Code	DQPSK	2 Mbps
	CCK	DQPSK	5.5 Mbps
	CCK	DQPSK	11 Mbps

802.11b

Coding Technique	Modulation Technology	Data Rate
OFDM	BPSK	6 Mbps
OFDM	BPSK	9 Mbps
OFDM	QPSK	12 Mbps
OFDM	QPSK	18 Mbps
OFDM	16QAM	24 Mbps
OFDM	16QAM	36 Mbps
OFDM	64QAM	48 Mbps
OFDM	64QAM	54 Mbps

802.11a

Роуминг

Роуминг – способность клиента переходить от одной ТД к другой, сохраняя соединение для приложений верхних уровней.

За принятие решения переходе на другую ТД отвечает клиентская сторона, при этом на новую ТД шлёт **REASSOCIATION** request:

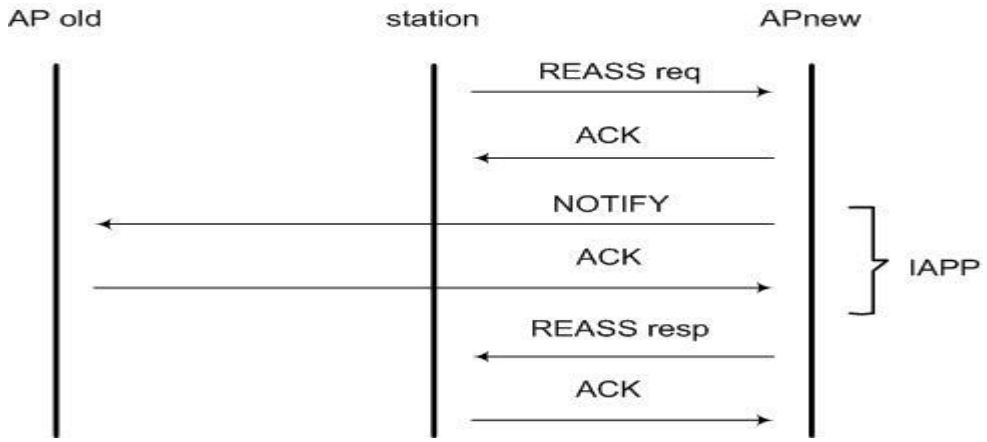
1. Клиент шлёт Reassociation request на APnew, в котором содержится SSID, MAC APold;

2. APnew отвечает ACK;

3. APnew связывается с APold, уведомляя её, что клиент пытается выполнить ассоциацию к ней. Данная процедура не описана в стандарте, существует IAPP, реализуемый каждым вендором по-своему;

4. При успешном соединении ТД APold шлёт ACK APnew;

Роуминг



5. APnew шлёт Reassociation response клиенту;

6. Клиент подтверждает ACK на APnew. Клиенту не обязательно отправлять Disassociation фрейм на APold, т.к. подразумевается, что APold и APnew успешно обменялись фреймами 3 и 4 через среду передачи (distribution system medium).

Благодарим за просмотр!

Наш адрес:

115419, Россия, Москва
ул. Орджоникидзе, 11, стр.1а

Телефон: **+7 495 641 40 45**
Факс: **+7 495 641 40 48**

vyvy@nstel.ruvy@nstel.ru www.nstel.ru
yvv2003@rambler.ru