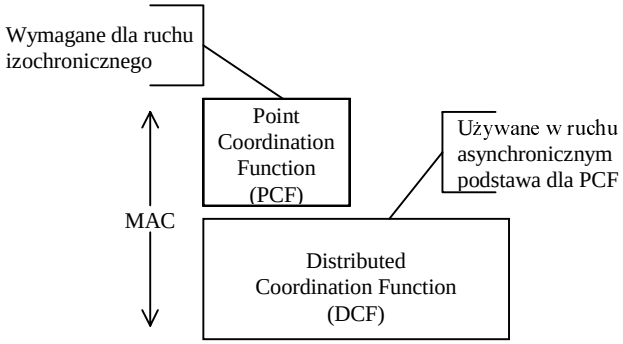
3. Standard IEEE 802.11.

Protokół DFWMAC (*Distribution Foundation Wireless Medium Access Protocol*) jest protokołem warstwy łącza danych modelu OSI/ISO. Jest on częścią większej rodziny protokołów tworzących razem bezprzewodową sieć LAN. Został on zaprojektowany z myślą o współpracy z różnymi konfiguracjami sieci standardu 802.11 i może realizować różne typy usług transferu danych.

3.1 Architektura

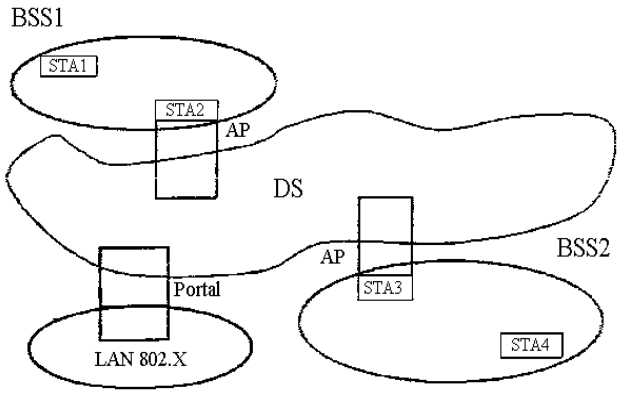
Protokół 802.11 jest tak skonstruowany, aby wszystkie funkcje realizowane od warstwy LLC (*Logical Link Control*) wzwyż były takie jak w innych sieciach LAN 802 (rys.8). Tak więc wszystko co związane jest z dostępem do medium musi być realizowane w warstwie fizycznej i warstwie MAC (*Medium Access Control*).



Rys. 8 Architektura IEEE 802.11 w odniesieniu do warstw ISO/OSI

Podstawową jednostką topografii sieci jest obszar, wewnątrz którego realizowana jest łączność bezprzewodowa. Obszar ten nazywa się BSA (*Basic Service Area*). Wszystkie urządzenia nadawczo-odbiorcze wewnątrz jednego BSA tworzące tzw. BSS (*Basic Service Set*) słyszą się nawzajem i są razem logicznie skojarzone. Przyłączenie do infrastruktury sieciowej opartej na łączności przewodowej (np. *Ethernet*) - realizowane jest przez komputer - punkt dostępu przyłączony do sieci kablowej i równocześnie posiadający komplet urządzeń zapewniających łączność bezprzewodową. Komputer ten w terminologii anglosaskiej nazywa się AP (*Access Point*), a sieć z funkcjonującym komputerem AP to sieć z infrastrukturą (*Infrastructure Network*). Komputer AP pełni również funkcje zarządzania siecią:

- uwierzytelnienie (legalizacja użytkowników) oraz funkcje kojarzenia poruszających się stacji bezprzewodowych z odpowiednimi BSA;
- bardzo ważne dla stacji niestacjonarnych funkcje zarządzania energią - zapamiętywanie, które stacje przechodzą w odpowiednie tryby energooszczędne, a także buforowanie ramek;
- synchronizacja stacji do wspólnego zegara.



Rys. 9 Topologia sieci standardu 802.11

Jednym z ograniczeń sieci bezprzewodowej jest mały zasięg działania. Pokrycie większego obszaru realizuje się tu poprzez wykorzystanie innej sieci DS. (*Distribution System*, rys. 9), opartej na przykład na kablu (ale niekoniecznie - może to być również sieć bezprzewodowa), kilku komputerów AP i stworzeniu wokół każdego z nich sieci bezprzewodowej LAN. Taki poszerzony obszar nazywa się ESA (*Extended Service Area*), a

urządzenia łączności bezprzewodowej tworzą ESS (*Extended Service Set*). Adresy są logicznie rozpoznawane poprzez odpowiednie identyfikatory: BSS-ID oraz ESS-ID. Komputery z kilku BSS mają wspólną cechę - dla warstwy LLC wyglądają jak pojedyncza sieć LAN - i przemieszczenie się w ramach jednego ESS pomiędzy kilkoma BSS jest operacją przeźroczystą dla warstwy LLC. Generalnie, kilka BSS może się zarówno pokrywać jak i być rozłączne. Do integracji z tradycyjnymi sieciami LAN służą tzw. „Portale" - obiekty logiczne - punkty, w których ramki z sieci innej niż 802.11 wchodzą do DS i w przeciwnym kierunku - dokonywana jest tu integracja pomiędzy sieciami 802.11 a kablowymi.

Nie zawsze jednak musi istnieć punkt dostępu do sieci opartej na kablu. Gdy brakuje takiego komputera, stacje sieci standardu 802.11 potrafią stworzyć sieć *Ad Hoc* (lub inaczej IBSS - *Independent Basic Service Set*), w której wspólnie dzielą się funkcjami synchronizacji.

Jeżeli chodzi o DS to standard nie precyzuje jaka to ma być sieć. Zamiast tego definiowane są usługi, które muszą być przez DS realizowane. Rozróżniane są dwie kategorie usług: *Station Services* i *Distibution System Services*. Do I kategorii zaliczane są usługi zapewniające transport ramek MSDU (*Message Service Data Units*) pomiędzy stacjami wewnątrz BSS, uwierzytelnienie stacji do sieci, anulowanie uwierzytelnienia oraz usługa szyfrowania danych. Do II kategorii usług zaliczane są usługi pozwalające na doręczanie ramek pomiędzy różnymi BSS poprzez *Distribution System*. Należą do nich: przyłączenie stacji do sieci (do AP), odłączanie, przełączanie do innego AP, zarządzanie przenoszeniem ruchu poprzez DS oraz przenoszenie ruchu pomiędzy *Distibution System* a sieciami kablowymi poprzez portale.

Parametry urządzeń i sieci 802.11	
Częstotliwość pracy / moc	2400-2483.5 MHz / 0.1W (20 dBm) Europa 2400-2483.5 MHz / 1W (30dBm) USA 850-950 nm
Pasmo przenoszenia	80 MHz
Prędkość transmisji	1, 2 Mb/s
Komunikacja	Bezpołączeniowa
Topologia sieci	- ad hoc - oparta o infrastrukturę
Maksymalny zasięg	20 - 50 m wewnątrz budynków kilkaset metrów na otwartej przestrzeni
Moc pobierana	Do kilkuset mW
Modulacja	Z rozproszonym widmem (direct sequence DBPSK, DQPSK z rozproszonym widmem (frequency hopping) 2GFSK, 4GFSK BT=0.5
Dostęp do kanału	CSMA/CA, RTS/CTS, PCF
Czułość odbiornika	Większa niż –80 dBm dla 1Mb/s Większa niż –75 dBm dla 2Mb/s
Stopa błędów	Lepsza niż 10^{-5}

Tabela 3 Parametry sieci 802.11.

3.2 Warstwa fizyczna

Wykorzystywanym pasmem jest pasmo ISM (*Industrial, Scientific and Medical Applications*). Są to trzy pasma częstotliwości: 902-928 MHz, 2400-2483.5 MHz i 5725-5850 MHz. Są to częstotliwości przeznaczone do wykorzystania przez aplikacje przemysłowe, naukowe i medyczne z wyłączeniem telekomunikacyjnych. Typowym zastosowaniem są tu przemysłowe urządzenia grzewcze, kuchenki mikrofalowe, automatyczne urządzenia lokacyjne i telefony bezprzewodowe. Standard 802.11 wybrał pasmo 2400-2483.5 MHz z uwagi na jego dostępność w takich krajach jak: USA, Wielka Brytania, kraje Europy Zachodniej (w tym również Polska) oraz Japonia. Szerokość pasma - ponad 80 MHz pozwala na realizację komunikacji o dużych przepływnościach, a implementacja urządzeń jest prostsza i bardziej efektywna niż urządzeń przeznaczonych dla częstotliwości o kilka GHz większych. Poza tym specjalnie dla pasm ISM zostały zaprojektowane nowe technologie radiowe - rozproszonego widma sygnału (S*pread Spectrum*). Standard 802.11 zezwala na wykorzystanie dwóch rodzajów techniki rozproszonego widma: DSSS (*Direct Sequence Spread Spectrum*) oraz FHSS (*Frequency Hopping Spread Spectrum*). Jeżeli chodzi o moc nadajników, to w warunkach europejskich nie może ona przekraczać 100mW (znacznie mniej niż warunki amerykańskie), co gwarantuje działanie systemu w zasięgu 20-50m w pomieszczeniach zamkniętych oraz kilkaset metrów na zewnątrz budynków.

W DSSS wykorzystywana jest modulacja BPSK (dwuwartościowa modulacja *Phase Shift Keying*) lub QPSK (czterowartościowa modulacja *Phase Shift Keying*). Otrzymuje się tu przepływności odpowiednio rzędu 1 lub 2 Mbit/s. Pasmo podzielone jest na 5 podpasm o szerokości 26 MHz każde. Środkowe częstotliwości tych podpasm wynoszą: 2412, 2427, 2442, 2457 i 2470 MHz. Jak widać część z tych pasm częściowo się pokrywa. Z kolei technologia FHSS dzieli kanał na 79 podpasm o szerokości 1 MHz każde. Do dyspozycji użytkownika są

trzy sekwencje złożone z 22 „*hops*”. Ten standard zapewnia bardzo efektywne wykorzystanie czasu i częstotliwości, wykazujące swoją przydatność szczególnie podczas retransmisji ramek.

W standardzie 802.11 można również wykorzystać technologię DFIR (*Diffussed Infra Red*). Przy wykorzystaniu tu modulacji OOK (*On-Off Keying*) otrzymuje się przepływność rzędu 1 Mbit/s. Produkty wykorzystujące DFIR pracują w pasmie 18-19 GHz, licencjonowanym przez FCC (*Federal Communication Commision*), bądź wykorzystują pasma *ISM* pracując z niską mocą. Porównanie technologii pokazane jest w Tabeli 4.

Technologia	DFIR	DSSS	FHSS
Przepływność (Mb/s)	1-4	2-20	1-3
Możliwość poruszania się stacji	stacjonarne/ ruchome	Stacjonarne/ Ruchome	ruchome
Zasięg [m]	15 – 65	30 - 270	30 -100
Długość fali / częstotliwość	800 – 900nm	Pasmo ISM	pasmo ISM
Modulacja	OOK	QPSK	GFSK
Moc emitowana		< 1W	< 1W
Metoda dostępu	CSMA	CSMA	CSMA

Tabela 4 Porównanie technologii przesyłania sygnału

Technika rozproszonego widma, polegająca na kodowaniu sygnałów radiowych stosowana najpierw w urządzeniach militarnych, a następnie w systemach telefonii komórkowej GSM, jak również w lokalnych sieciach bezprzewodowych, ma na celu zwiększanie odporności na zagłuszanie (przy nadawaniu) oraz przeciwdziałanie zanikom (przy odbiorze) transmitowanych sygnałów cyfrowych. Technika szerokiego pasma SS obejmuje wiele metod rozpraszania widma, z których najczęściej są stosowane:

- metoda FH *(Frequency Hopping)* polegająca na skokowej zmianie częstotliwości nośnych według uprzednio uzgodnionego pseudolosowego klucza kodowego między stacją nadawczą i odbiorczą, zmieniającego się w trakcie transmisji. Metoda ta nie wymaga angażowania urządzenia centralnego kierującego pracą sieci i uzgadniania zezwoleń na zajmowanie kanałów radiowych. System odbiorczy stosuje synchronicznie taki sam pseudolosowy algorytm "przeskakiwania" częstotliwości jak urządzenie nadawcze, zmniejszając wpływ zakłóceń występujących na dyskretnych częstotliwościach radiowych;
- metoda DS *(Direct Sequence)* polegająca na zmianie fazy w strumieniu bitów danych przez zmieszanie informacji z pseudolosowym kodem rozpraszającym, znanym wyłącznie stacji nadawczej i odbiorczej. Operacja ta powoduje rozproszenie sygnału informacyjnego w szerokim paśmie częstotliwości, przypominającego biały szum, trudno wykrywalny na tle naturalnych szumów radiowych. Wielokrotne kodowanie tej samej informacji (bity, bajty, pakiety) umożliwia nawet transmisję wiadomości poniżej szumów radiowych.

3.3 Metody dostępu.

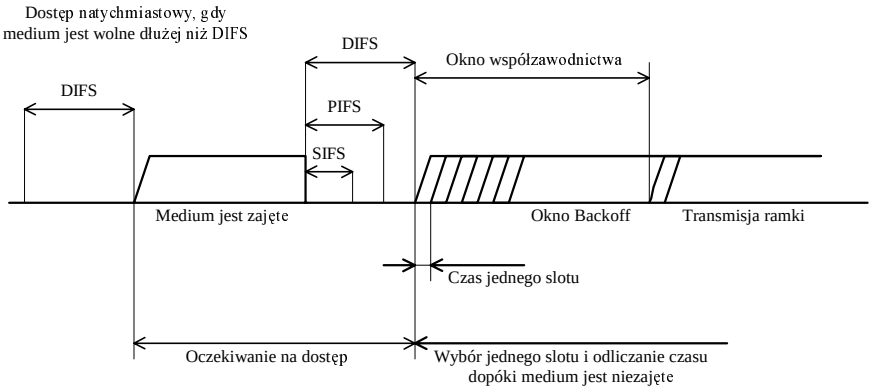
W standardzie 802.11 proponowane są dwa typy usług transferu: asynchroniczne i izochroniczne. W sieci z infrastrukturą (obecny komputer punktu dostępu - AP), możliwa jest implementacja usług izochronicznych. Komputer AP zarządza podziałem dziedziny czasu na szczeliny czasowe oraz podziałem tej szczeliny na część w której następuje realizacja usług izochronicznych - wtedy zarządzanie działaniem sieci jest zcentralizowane - całą siecią zarządza komputer AP. Pozostała część szczeliny wykorzystywana jest na ruch asynchroniczny - zarządzaniem kolejnością transferu zajmują się wszystkie stacje - zarządzanie staje się rozproszone. W sieci *Ad Hoc* (brak komputera AP) nie istnieje odgórny podział na szczeliny czasu i istnieje tylko zarządzanie rozproszone, realizujące ruch asynchroniczny - tak więc usługi izochroniczne są opcjonalne tylko dla sieci z infrastrukturą i protokół potrafi działać także bez nich.

Metodą dostępu do sieci jest CSMA/CA (*Carrier Sense Multiple Access / Collision Avoidance*). Każda stacja, przygotowana do transmisji, nasłuchuje medium, sprawdzając czy jakaś inna stacja właśnie nie transmituje. Jeżeli medium nie jest zajęte, przystępuje do transmisji, w przeciwnym wypadku oczekuje na zakończenie bieżącej transmisji. Następnie wybiera pewien przedział czasu, po którym zamierza przystąpić do transmisji, ciągle nasłuchując medium. Jeżeli medium do tego czasu nie zostało zajęte, zaczyna się transmisja. Oczywiście możliwe jest, że jakaś inna stacja przystąpi w tej samej chwili do transmisji. Wtedy następuje kolizja, o której stacje dowiadują się poprzez mechanizm potwierdzeń, co powoduje podjęcie kroków powodujących retransmisję.

W DFWMAC znajdują się dwie funkcje zarządzające przebiegiem transmisji: rozproszona DCF (*Distributed Coordination Function*) i zcentralizowana PCF (*Point Coordination Function*). Ta druga może być

zaimplementowana jako opcja tylko w sieci z infrastrukturą, implementacja pierwszej jest obowiązkowa w każdej konfiguracji (*Ad Hoc* oraz z infrastrukturą). Oprócz tego, sieć z zaimplementowaną funkcją PCF nie może pokrywać się z inną taką siecią pracującą na tym samym kanale, wymagana jest więc wystarczająca izolacja pomiędzy kilkoma sąsiednimi PCF, lub używanie kilku kanałów pracy w przypadku sieci ESS, ewentualnie ograniczenie użycia funkcji PCF tylko do jednego BSS. Sposób dostępu do sieci CSMA/CA jest wzbogacony o mechanizm wirtualnego nasłuchiwania i rezerwacji medium do transmisji - Virtual CS (*Virtual Carrier Sense*) / NAV (*Net Allocation Vector*). Otóż ramki przenoszą w nagłówkach informacje, dzięki którym inne stacje wstrzymują się od prób zajmowania sieci przez pewien czas w przyszłości. Każda stacja nasłuchując przez cały czas medium, uaktualnia swoje wartości NAV rezerwując medium na przyszłość. Zanim przystąpi do transmisji bierze ona pod uwagę wartość NAV traktując go równoprawnie z faktycznym stanem zajęcia medium. W protokole DFWMAC wyróżnia się 3 istotne przedziały czasowe: SIFS, PIFS, DIFS (*Short-, PCF-, DCF- Inter Frame Space*, o zależnościach DIFS>PIFS>SIFS). Odmierzane są one przez każdą stację od chwili zakończenia zajętości medium i służą do określenia czasu rozpoczęcia nadawania przez daną stację. W protokole są ustalone również trzy rodzaje priorytetów transmisji, zależne od tych przedziałów (rys. 10).

- Priorytet DCF. Jest on używany do nadawania ramek asynchronicznych w tzw. oknie współzawodnictwa (*Contention Window* - po upływie przedziału DIFS od ostatniej zakończonej transmisji następuje okno czasowe, podzielone na pewną ilość szczelin czasowych o równej długości, w których stacja może rozpocząć nadawanie). Po upływie czasu DIFS od momentu, gdy funkcja monitorowania sieci stwierdzi, że medium nie jest zajęte, a wektor alokacji sieci NAV nie jest ustawiony, mogą zostać nadane ramki RTS (*Request To Send*) lub DATA (dane);
- Priorytet PCF. Jest on używany przez stację AP, gdy zarządzanie przejmuje funkcja dostępu zcentralizowanego (PCF). Komputer AP może po upływie czasu PIFS (jest on krótszy od DIFS) od zwolnienia medium nadać przygotowane u siebie do transmisji ramki. Przywilej nadawania zarezerwowany jest tylko dla stacji AP, a transmisja przy użyciu dostępu scentralizowanego odbywa się niezależnie od transmisji z priorytetem DCF;
- Priorytet „*Short*". Jest przeznaczony dla wszystkich transmisji, ramek będących odpowiedziami na jakiś inną ramkę lub jej potwierdzeniem. Transmisja z tym priorytetem odbywa się po czasie SIFS (krótszym od PIFS) od chwili zwolnienia medium.



Rys. 10 Zależności pomiędzy czasami IFS

Stacja przystępująca do transmisji z priorytetem DCF czeka, aż medium będzie wolne przez czas *DIFS*. Następnie oblicza tzw. *Backoff* - szczelinę czasową w której rozpocznie transmisję. *Backoff* jest wybierany losowo (w pewnych granicach) i służy zrównoważeniu szans dostępu dla nadających stacji. Następnie wartość *Backoff* jest zmniejszana wraz z upływem czasu. Jeżeli przed upływem całego okresu *Backoff* zacznie nadawać inna stacja, odliczanie zostaje zawieszone aż do wykrycia następnego okresu DIFS.

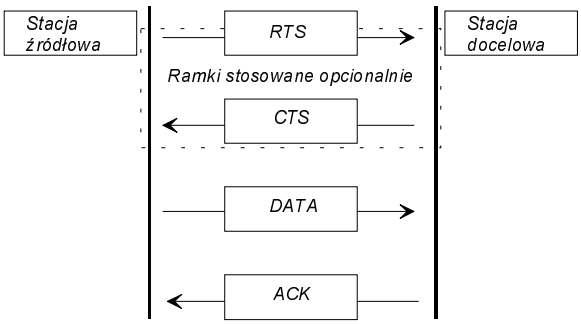
Gdy stacja zakończy odliczać *Backoff* rozpoczyna nadawanie. Ma do wyboru trzy różne warianty transmisji:

- Transmisja ramki przy użyciu opcji RTS/CTS (*Request To Send/Clear To Send*). Po czasie DIFS, po procedurze *Backoff* zostanie nadana ramka RTS. Jest to ramka przygotowująca pozostałe stacje na to, że kolejna ramka pochodząca od nadawcy ramki RTS będzie prawdopodobnie dłuższa od pewnego progu będącego parametrem sieci; zapobiega ona próbom nadawania przez inne stacje, dokonywana jest w ten sposób alokacja czasu na transmisję danej ramki. Nadawca przed upływem czasu T1 oczekuje przesłania od odbiorcy ramki CTS, potwierdzającej otrzymanie RTS. Jeżeli ramka CTS zostanie odebrana przed upływem

czasu T1, to po najbliższym czasie SIFS zostaje nadana właściwa ramka DATA (z danymi), a nadawca rozpoczyna odliczanie innego licznika - T3 (*Timer 3*) - oczekując na przysłanie potwierdzenia ACK (*Acknowledgement*) od adresata. Jeżeli nadawca nie otrzyma właściwych odpowiedzi po czasie T1 lub T3 następuje procedura retransmisji. Istotne są informacje jakie niosą w sobie ramki RTS i CTS. Otóż znajdują się tam dane, powodujące rezerwację medium na pewien okres czasu. Informacja z ramki RTS jest powtórzona w ramce CTS - dzięki temu w przypadku, gdy część stacji jej nie usłyszy (tzw. „*hidden stations*"), mają one szansę usłyszeć ją z ramki CTS;

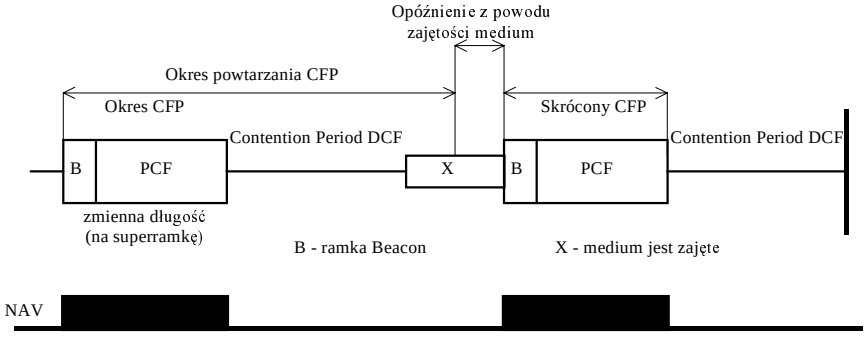
- Transmisja ramki bez użycia opcji RTS/CTS. Po czasie DIFS, po procedurze *Backoff* zostanie nadana ramka DATA. Następnie zostaje uruchomiony licznik T3 (*Timer 3*) nadawcy. Nadawca przed upływem czasu T3 oczekuje przesłania od odbiorcy ramki potwierdzenia ACK. Jeżeli nadawca nie otrzyma właściwej odpowiedzi następuje procedura retransmisji;
- Transmisja ramki w trybie *Broadcast/Multicast* (do wszystkich lub niektórych stacji). Po czasie DIFS, po procedurze *Backoff* zostanie nadana ramka DATA. Nie są przesyłane żadne potwierdzenia.

Schemat przykładowej wymiany ramek został pokazany na rysunku 11.



Rys. 11 Przykładowa wymiana ramek między stacją źródłową i docelową.

Powyższe usługi asynchroniczne, to usługa *Contention Service* (ang. od współzawodnictwa transmisji w oknie *Contention Window*). Oprócz tego, w implementacji sieci z infrastrukturą, możliwe są usługi CFS (*Contention Free Services*). Wykorzystują one zcentralizowane zarządzanie dostępem do sieci. Połączenie *PCF* i *DCF* dokonywane jest poprzez stworzenie tzw. superramki (ang. *SuperFrame*). Cała dziedzina czasu dzielona jest na superramki - zajmuje się tym stacja AP. Okresowo generuje ona specjalne ramki (zw. „*Beacons*") niosące informację o zajętości medium dla potrzeb metody dostępu PCF. Dane przenoszone w tych ramkach powodują ustawienie wektora NAV na początku każdej superramki. Z kolei każda superramka podzielona jest na pole przeznaczone dla usług CFS (o zmiennej długości), pozostałą część zajmują normalne usługi zarządzane w sposób rozproszony DCF (rys. 12).



Rys. 12 Contention Free Period i Contention Period

Na początku każdej superramki kontrolę nad medium przejmuje PCF. Może się zdarzyć, że medium jest zajęte - oznacza to, że trwa jeszcze fragment transmisji DCF z poprzedniej superramki - wtedy procedury PCF są opóźniane (*SuperFrame Stretching*) aż do zakończenia transmisji, ale czas trwania superramki nie jest modyfikowany. W trakcie działania funkcji dostępu PCF następują transmisje oparte na schemacie pollingu (przepytywania). Stacje, które dostały wcześniej przywilej pracy w okresie PCF (mogły to zrobić generując

odpowiednią ramkę z żądaniem umieszczenia ich na liście stacji przepytywanych podczas rozproszonego dostępu do medium) zostają umieszczone na liście przepytywania i są kolejno wywoływane przez stację AP. Należy jeszcze dodać, że maksymalny przedział czasu przeznaczony na usługi CFS jest ograniczony przez maksymalny czas trwania ramki dla ruchu DCF wg. wzoru:

Górna_granica_czasu_na_usługę_CFS = Czas_Superramki - Max._długość_ramki_asynch.

Oznacza to, że w każdej superramce musi być czas przeznaczony dla usługi asynchronicznej w oknie współzawodnictwa o długości umożliwiającej przesłanie co najmniej ramki z danymi.

3.4 Synchronizacja.

Wszystkie stacje wewnątrz danego BSS powinny być zsynchronizowane. Procedury synchronizacji są używane do funkcji zarządzania poborem mocy stacji (oszczędzanie baterii), zarządzaniem warstwą fizyczną - *Frequency Hopping* oraz do ramkowania usług izochronicznych CFS. Procedurami synchronizacji w każdej stacji zajmuje się funkcja TSF (*Timing Synchronization Function*).

W sieci z infrastrukturą, synchronizacja sieci należy do obowiązków stacji AP. Wysyła ona okresowo ramki „*Beacon*", zawierają kopię wskazania jego własnego zegara. Pozostałe stacje zawsze akceptują otrzymaną ramkę i dokonują uaktualnienia swojego zegara.

W sieciach *Ad Hoc*, pozbawionych stacji AP zarządzającym synchronizacją, używany jest rozproszony algorytm synchronizacji. Wszystkie stacje dzielą odpowiedzialność za utrzymywanie synchronizacji pomiędzy sobą. Każda stacja ma swój zegar TSF, używany do odmierzania momentów TBTT (*Target Beacon Transmission Time*), w których oczekiwane jest zsynchronizowanie zegarów. W chwili TBTT, każda stacja zaczyna odmierzanie losowego czasu. Jeżeli w chwili zakończenia odmierzania tego czasu medium jest zajęte, stacja oczekuje do jego zwolnienia. Jeżeli okaże się, że w chwili zwolnienia medium i po odczekaniu wybranego wcześniej losowo przedziału do stacji nie dotarła ramka *Beacon* od innej stacji, wysyła swoją ramkę *Beacon*. Zawiera ona min. dane o wskazaniu własnego zegara. Nie zawsze jednak odebrana ramka *Beacon* od innej stacji jest akceptowana - ramka jest akceptowana tylko wówczas, gdy zawarte w niej wskazania zegara mają większą wartość niż w odbierającej stacji.

3.5 Zarządzanie poborem energii.

Mechanizm zarządzania poborem mocy w sieci 802.11 pozwala na pełnoprawną pracę stacji w sieci z wyłączonym przez pewną część czasu zasilaniem. Urządzenia nadawczo-odbiorcze stacji mogą przebywać w dwóch stanach:

- Czuwanie (*Awake*) - odbiornik pracuje pełną mocą - odbiór lub oczekiwanie na odbiór;
- Drzemka (*Doze*) - stacja nie może nadawać i odbierać - zużywa bardzo mało energii, niektóre obwody są jednak aktywne (np. liczniki).

Standard IEEE 802.11 definiuje dwa sposoby zarządzania poborem energii: dla infrastruktury (obecny punkt dostępu) i dla sieci ad-hoc.

Sieć z infrastrukturą

W przypadku sieci z infrastrukturą drzemiące stacje periodycznie budzą się i nasłuchują wybranych ramek *Beacon* wysyłanych przez punkt dostępu. Jeżeli stacja usłyszy ramkę kontrolną wskazującą, że punkt dostępu posiada w buforze dane przeznaczone dla niej, wysyła specjalną ramkę *Poll*, która nakazuje punktowi dostępu wysłać kolejkowane do niej dane.

Sieć Ad Hoc

Działanie mechanizmów zarządzania poborem energii jest podobne jak w przypadku sieci z infrastrukturą. Stacje będące w danej komórce budzą się na krótki, zdefiniowany wcześniej okres czasu by usłyszeć czy powinny przygotować się do odbioru ramki.

3.6 Uwierzytelnianie i szyfracja

W sieciach bezprzewodowych medium jest współdzielone przez wszystkie stacje mające nadajniki i odbiorniki. Ta dowolność w uzyskaniu dostępu do sieci zmusza do szukania środków zastępczych, ograniczających i kontrolujących dostęp do medium. Służy do tego specjalna usługa realizowana w sieci standardu 802.11 - uwierzytelnienie. Należy ona do grupy usług *Station Services* - realizujących transmisję ramek pomiędzy stacjami w BSS. Przy jej pomocy stacje określają swoją tożsamość w kontaktach z innymi

stacjami i aby mógł nastąpić drugi krok przyłączenia do sieci - skojarzenie z konkretnym BSS - musi nastąpić obustronne uwierzytelnienie.

Standard 802.11 zostawia wybór przyszłym użytkownikom sieci, jeżeli chodzi o standard realizujący uwierzytelnienie w wyższych warstwach modelu ISO/OSI. Skupia się raczej na uwierzytelnianiu warstwy LLC. Uwierzytelnienie w tym wypadku oznacza sprawdzenie, czy transmitowane dane spełniają zakładane standardy warstwy fizycznej - a więc proces ten jest niezależny od innych algorytmów uwierzytelnienia realizowanych w warstwach wyższych. Dostarczane są dwa mechanizmy: pierwszy to właściwie jego brak - wszystkie stacje chcące przyłączenia do sieci są przyłączane, drugi - *Shared Key* - wymaga posiadania przez strony udowadniające swoją tożsamość odpowiedniego klucza. Opcja ta wymaga użycia WEP (*Wireless Equivalent Privacy*) - algorytmu szyfrującego, zawartego w standardzie 802.11.

Szyfrowanie danych należy do grupy usług typu *Station Services*. Szyfrowane mogą być tylko ramki danych oraz niektóre ramki zarządzające. Jak wspomniano powyżej, do szyfrowania używa się algorytmu WEP. Bloki danych poddawane są operacji XOR z pseudolosowym kluczem - algorytm przypomina DES *(Data Encryption Standard)* elektroniczna książka kodowa

Nadawca losuje 32 bitowy wektor inicjalizacji (IV). Przy pomocy tego wektora, tajnego klucza i algorytmu RSA RC4 generowany jest klucz kodujący. Z tekstu oryginalnego wyliczana jest najpierw 32 bitowa suma kontrolna, a następnie szyfrowany jest on poprzez poddanie go operacji XOR. Do odbiorcy przesyłane są: wektor inicjalizacji, zaszyfrowany tekst i suma kontrolna pozwalająca odbiorcy stwierdzić czy nie nastąpiła utrata integralności danych. U odbiorcy operacja ta jest odwracana. Klucz sesyjny otrzymywany jest przy pomocy wektora inicjalizacji, suma kontrolna wyliczana jest z odszyfrowanego tekstu i porównywana z nadesłaną. Jeżeli są identyczne, oznacza to, że wszystko przebiegło pomyślnie.