SPIS TREŚCI

1 Wprowadzenie

W historii rozwoju bezprzewodowej komunikacji mobilnej można wyróżnić trzy okresy. Pierwszy z nich to okres teoretycznych badań, poszukiwań i wreszcie wykorzystania fal radiowych dla celów komunikacji. Okres drugi związany był z rozwojem technik i ewolucją sprzętu. Trzeci okres obejmuje upowszechnienie zastosowań bezprzewodowej radiowej komunikacji mobilnej.

W dotychczas projektowanych i wykorzystywanych systemach mobilnych realizowane są szeroko rozumiane usługi głosowe i usługi transmisji danych. Obszar głównego zainteresowania tj. usługi transmisji danych mogą być realizowane w dwóch typach systemów, które różnią się względem siebie zarówno zasadami funkcjonowania jak i obszarem dostępności usług. Pierwszy z systemów był pierwotnie przeznaczony dla świadczenia usług głosowych, natomiast drugi był rozwijany i optymalizowany pod kątem realizacji aplikacji związanych z transmisją danych. W chwili obecnej ze względu na kryterium obszaru (zasięgu) dostępności usług można mówić o dwóch typach sieci bezprzewodowych realizujących usług i aplikacji związanych z transmisją danych. Należą do nich lokalne sieci komputerowe o niewielkim zasięgu rzędu kilkuset metrów kwadratowych oraz sieci rozległe o dużym zasięgu - WAN.

Koncepcje zastosowania fal radiowych w bezprzewodowych sieciach lokalnych - WLAN (*ang. Wireless Local Area Network*) pojawiły się już w latach 1980. Duża atrakcyjność tego typu sieci wynikająca głównie z ich elastyczności i ekonomiczności spowodowała, że stały się wkrótce nowym, dynamicznie rozwijającym się segmentem rynku. Masowo zaczęły pojawiać się różnorodne rozwiązania sprzętowe oferowane i dostarczane przez wielu producentów, które jednak nie umożliwiały wzajemnej współpracy. Spowodowało to podjęcie prac standaryzacyjnych zarówno w Stanach Zjednoczonych i Japonii oraz w Europie.

Prace standaryzacyjne są prowadzone przez powszechnie znane organizacje zajmujące się normalizacją różnych aspektów telekomunikacji o zasięgu międzynarodowym, regionalnym i krajowym. Wiodącą organizacją międzynarodową jest ITU (*ang. International Telecommunication Union*). W odniesieniu do systemów bezprzewodowych podstawowym zadaniem tej organizacji jest zarządzanie widmem i podejmowanie działań regulacyjnych mających na celu minimalizację szkodliwego oddziaływania stacji radiowych z sąsiadujących ze sobą regionów. ITU-R jako specjalizowany organ ITU odpowiada za organizacyjno - techniczne aspekty współpracy systemów mobilnych oraz sieci publicznych oraz tworzenie standardów komunikacji radiowej. Rezultaty swojej działalności ITU-R ogłasza, co cztery lata w formie raportów i zaleceń.

Na terenie Europy koordynatorem działalności standaryzacyjnej w zakresie telekomunikacji jest CEPT (*ang. European Conference of Postal and Telecommunications Administrations*). Za obszar związany z komunikacją przy wykorzystaniu fal radiowych jest odpowiedzialny komitet ERC (*ang. European Radio Committee*). Trzy stałe grupy robocze tego komitetu wyniki prac publikują w postaci:

- raportów - koncentrują się one na wybranej tematyce lub wybranych zagadnieniach;
- zaleceń nie mają one charakteru obligatoryjnego;
- zaleceń obligatoryjnych - zalecenia, które muszą być respektowane i stosowane przez sygnatariuszy.

Ważnym ciałem standaryzacyjnym, z którym coraz ściślej współpracuje CEPT jest ETSI (ang. *European Telecommunications Standards Institute*), którego komitet techniczny (TC) tworzy i rozwija standardy europejskie. Standardy te są oznaczane jako ETS (*ang. European Telecommunications Standards*).

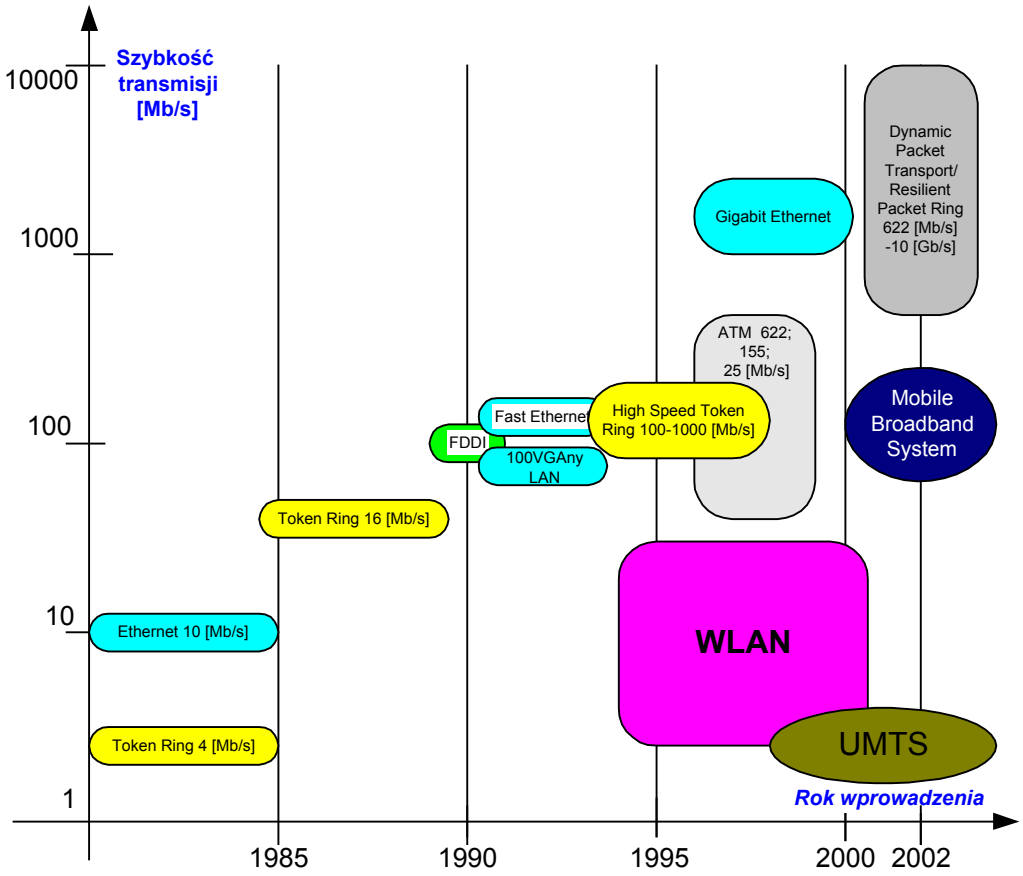
W Stanach zjednoczonych głównym koordynatorem prac standaryzacyjnych jest ANSI (ang. *American National Standard Institute).* Ważną w tym obszarze terytorialnym organizacją o charakterze naukowym jest IEEE (ang. *Institute of Electrical and Electronics Engineers*), której

komitet techniczny odpowiada w szczególności za rozwijanie i proponowanie standardów telekomunikacyjnych.

Wszystkie wymienione organizacje rozpoczęły opracowywanie standardów dla bezprzewodowych sieci lokalnych zakładając, że tego typu sieci powinny zapewniać komunikację o relatywnie dużej przepływności (min. 10 Mbit/s) użytkownikom przemieszczającym się z niewielkimi prędkościami liniowymi oraz kątowymi w ograniczonym obszarze np. na terenie budynku lub campusu. Ustalono, że bezprzewodowe sieci lokalne będą charakteryzowane następującymi parametrami:

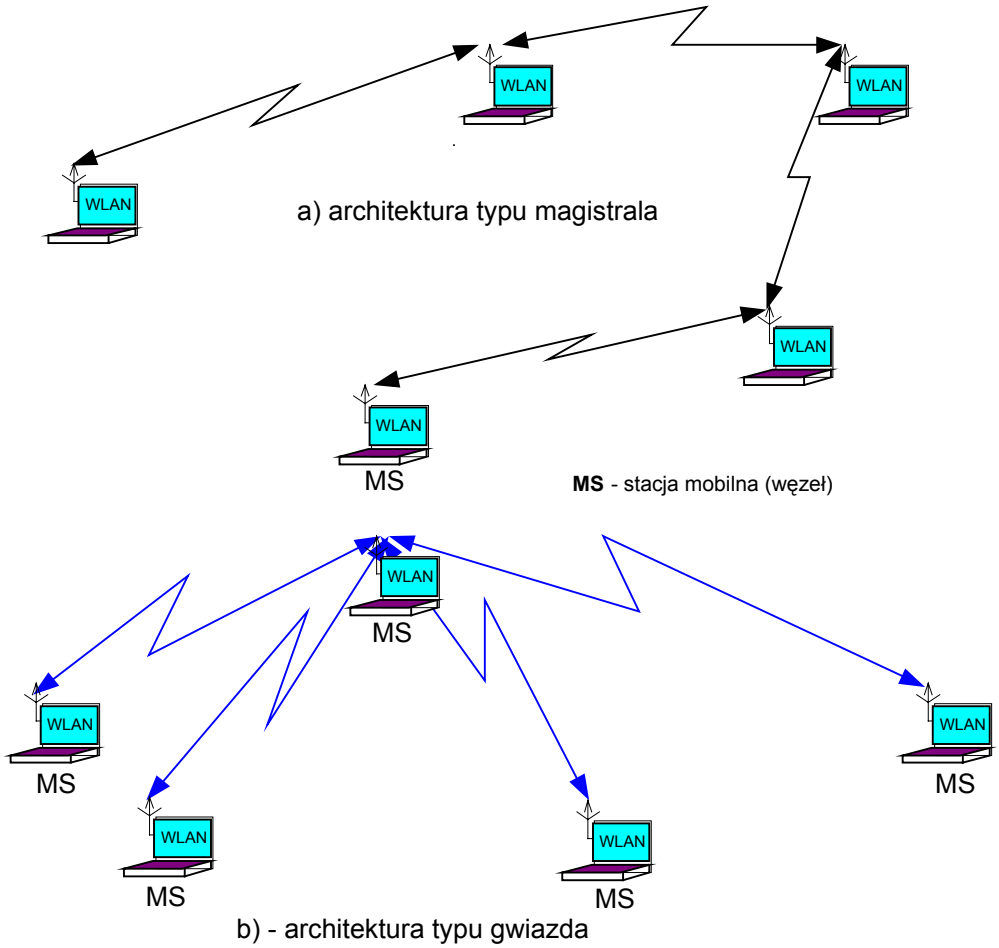
- uzyskiwana przepływność (jeden z głównych parametrów sieci WLAN);
- zestaw protokołów - pozwala określić stopień potencjalnych możliwości współpracy miedzy różnymi typami urządzeń i sieci;
- obszar (zasięg) dostępności usług sieciowych określanych także jako obszar pokrycia usługami;
- stopień bezpieczeństwa informacji przenoszonych w sieci;
- efektywność i oszczędność zużycia energii (energochłonność);
- poziom mocy nadawanych sygnałów.

W ramach rozwoju sieci bezprzewodowych, sieci WLAN można poglądowo umiejscowić w sposób przedstawiony na poniższym rysunku:



Rys. 1.1. Umiejscowienie sieci WLAN w kontekście ogółu sieci bezprzewodowych

Z punktu widzenia topologii sieciowych założono natomiast, że wykorzystywane będą jedynie dwa typy topologii tj. magistrala (odpowiednik konfiguracji Ethernet) oraz gwiazda, w której ruchem w sieci zarządza stacja centralna. Wymienione topologie zostały przedstawione na rys. 1.2.



Rys. 1.2. Podstawowe rodzaje topologii bezprzewodowych sieci lokalnych (WLAN).

W wymienionych typach sieci wykorzystywane są dwa typy medium (warstwa fizyczna) tj. fale optyczne z zakresu podczerwieni - IR (*ang. Infrared*) o długościach z zakresu od 10^{-4} do 10^{-6} m oraz fale radiowe w podzakresach:

- 902 - 908 MHz;
- 2,4 -2,5 GHz;
- 5 GHz;
- 5,8 - 5,96 GHz;
- 18 - 19 GHz.

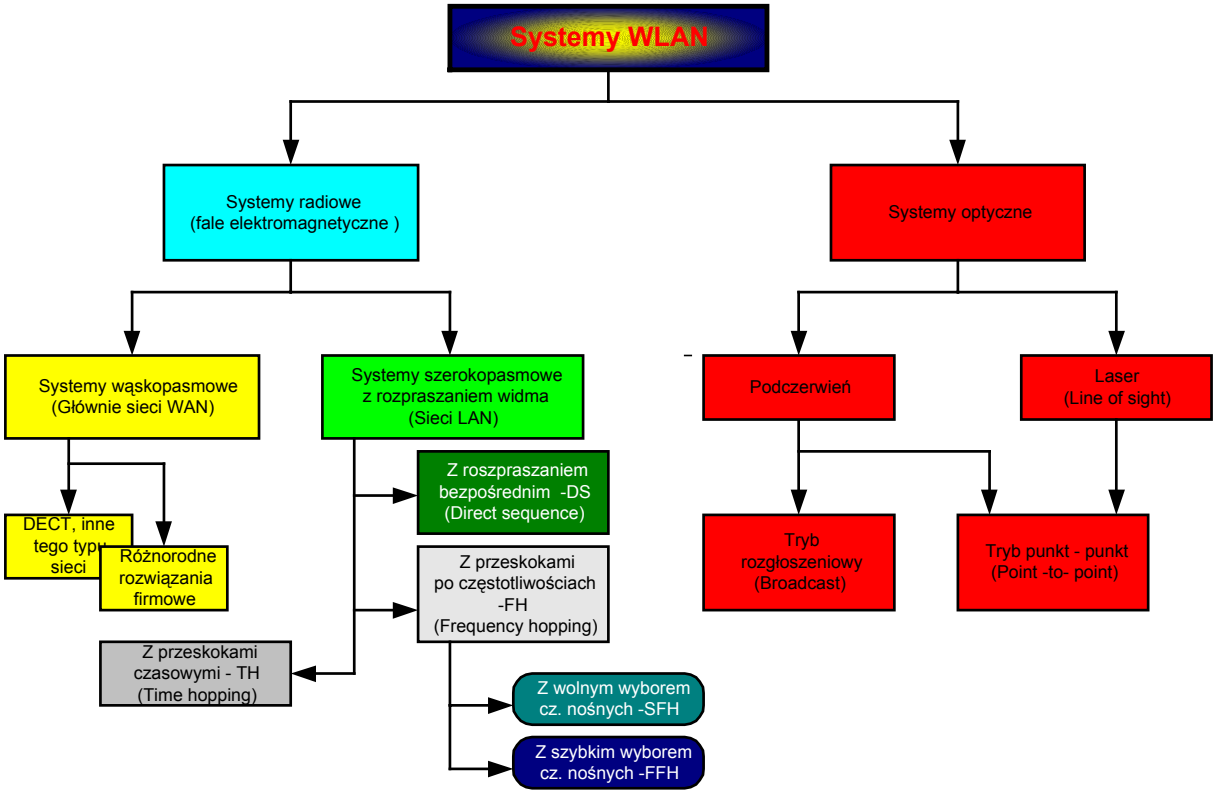
Warstwę fizyczną z wykorzystaniem fal optycznych zdecydowano się przeznaczyć dla aplikacji, w których nadajniki i odbiorniki znajdują się w bezpośredniej widoczności optycznej. Zastosowane rozwiązanie jest podobne do rozwiązań technicznych wykorzystywanych przy zdalnym sterowaniu funkcjami sprzętu elektronicznego (np. TV, video itp.).

Warstwę fizyczną z wykorzystaniem fal radiowych postanowiono realizować na dwa sposoby:

- z rozpraszaniem widma metodą kluczowania bezpośredniego - DSSS (*ang. Direct Sequence Spread Spectrum*);
- z rozpraszaniem widma metodą przeskoków częstotliwości - FHSS (*ang. Frequency Hopping Spread Spectrum*)[1].

Przeglądową kategoryzację systemów bezprzewodowych sieci lokalnych ze względu na stosowany rodzaj fal, ich zakres oraz technikę transmisji w formie graficznej przedstawiono na rys. 1.3.

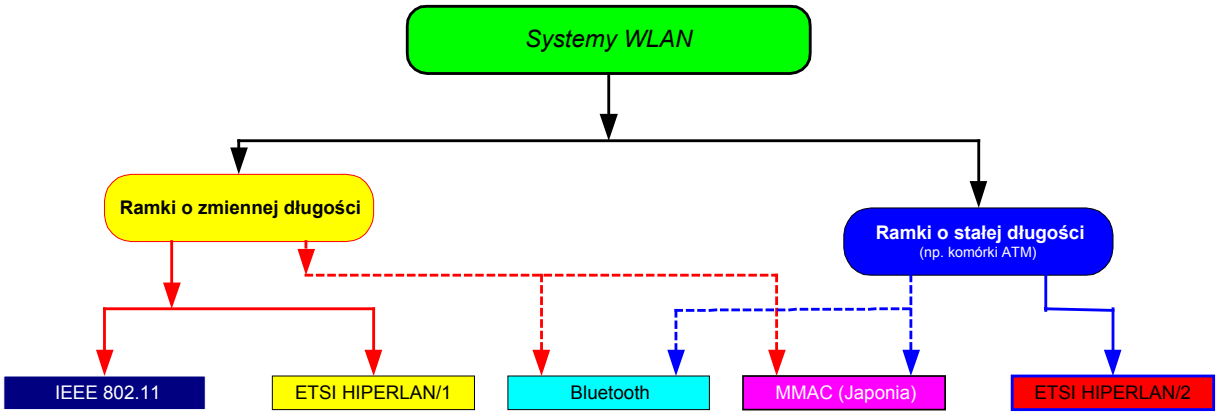
[1] *Istnieje także technika nazywana FT (ang. Frequent Time), która jednak posiada marginalne znaczenie.*



DECT - Udoskonalona telekomunikacja bezsznurowa (ang. Digital Enhanced Cordless Telekommunications)

Rys. 1.3. Kategoryzacja systemów bezprzewodowych sieci lokalnych (WLAN) ze względu na stosowany rodzaj fal, ich zakres oraz technikę transmisji.

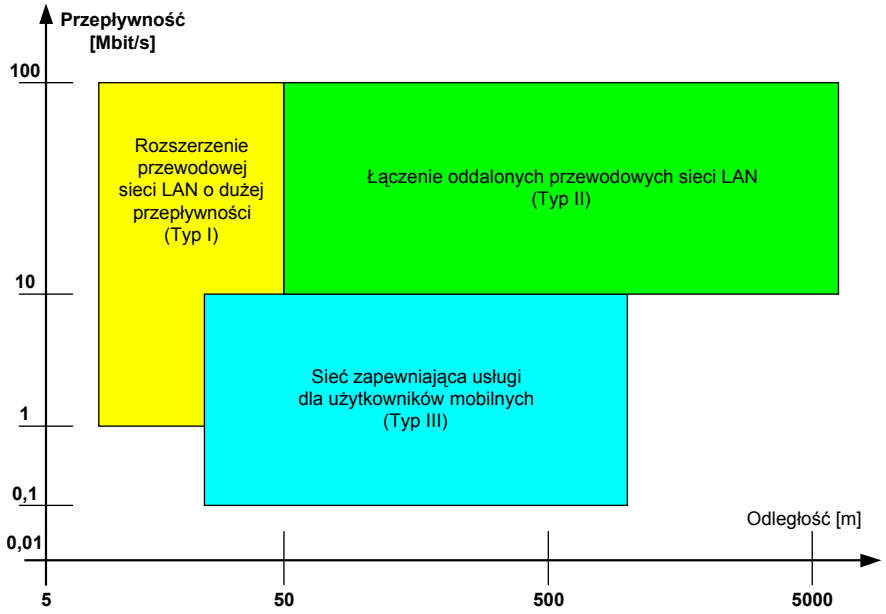
Innym stosowanym kryterium w kategoryzacji bezprzewodowych sieci lokalnych (WLAN) jest podział odzwierciedlający rodzaj stosowanych ramek, co przedstawiono na poniższym rysunku:



Rys. 1.4. Kategoryzacja systemów bezprzewodowych sieci lokalnych (WLAN) ze względu na rodzaje stosowanych ramek.

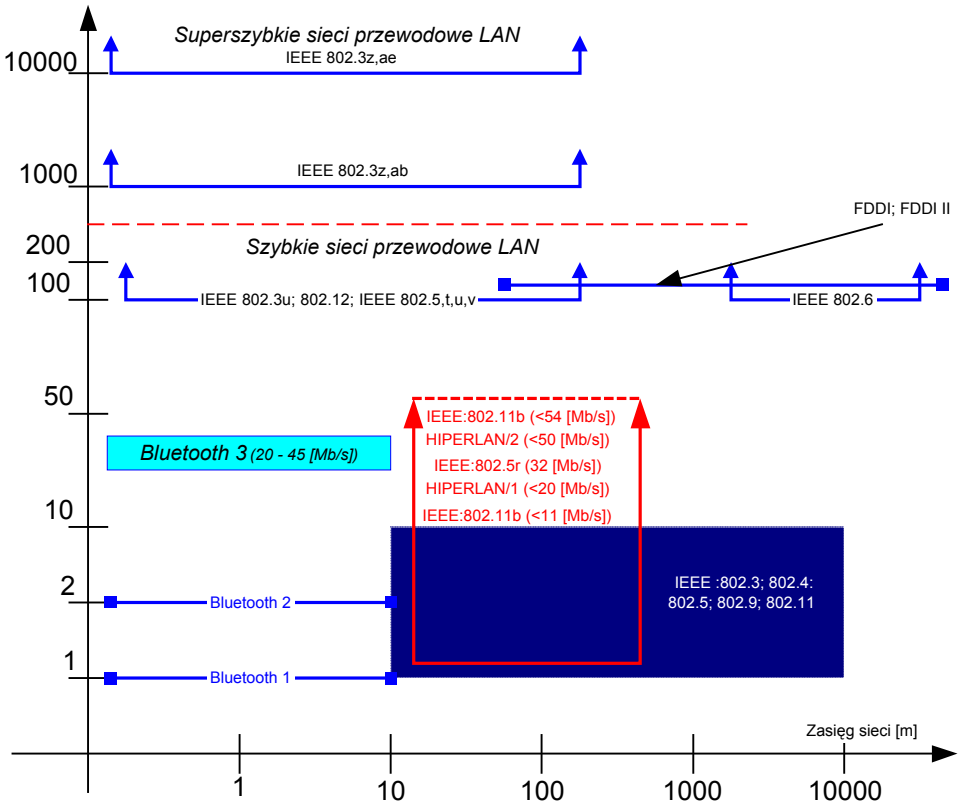
Przy określaniu sposobu wykorzystania sieci WLAN założono zasadniczo trzy główne obszary zastosowań. Jako główną i podstawową aplikację tej sieci przyjęto rozszerzenie zasięgu istniejących przewodowych sieci lokalnych LAN drogą umożliwienia dostępu do stacji mobilnych. W szczególności odnosi się to do obszarów, w których dodatkowa instalacja sieci przewodowej jest kłopotliwa np. w dużych halach produkcyjnych czy w obiektach zabytkowych, gdzie wprowadzenie okablowania może być niecelowe bądź nawet niedozwolone. Drugą przyjętą aplikacją jest łączenie sieci LAN umiejscowionych w różnych budynkach. Trzecim typem aplikacji jest realizacja usług związanych z transmisją danych dla użytkowników posługujących się komputerami przenośnymi i przebywający w szczególnego typu obszarze np. portu lotniczego, budynku hotelowego itp.

Na rysunku 1.5. przedstawiono przewidywane obszary zastosowań bezprzewodowych sieci lokalnych, ich przepływności oraz zasięg.



Rys. 1.5. Obszary zastosowań bezprzewodowych sieci lokalnych

Natomiast kolejny diagram przedstawia umiejscowienie sieci WLAN w otoczeniu wykorzystywanych obecnie sieci LAN, z uwzględnieniem najistotniejszych standardów, zasięgu oraz oferowanych szybkości transmisji.



Rys. 1.6. Porównanie możliwości sieci WLAN i klasycznych systemów LAN .

Na podstawie badań przeprowadzonych przez liczne ośrodki naukowo - badawcze zdefiniowano wymagania jakościowe dla wielu usług, które mogą być realizowane w sieciach WLAN. Przykłady wymagań przedstawiono w tabeli 1.1.

Tabela 1.1. Wymagania jakościowe dla wybranych usług sieci WLAN

Lp.	Rodzaj aplikacji	Wymagana przepływność [kbit/s]	Dopuszczalne opóźnienie transmisji [ms]	Dopuszczalna bitowa stopa błędów (BER)
1.	Telefonia	13 - 64	< 140	$< 3 \times 10^{-5}$
2.	Dźwięk wysokiej jakości	1400	< 500	$< 3 \times 10^{-5}$
3.	Videotelefonia	32 - 2000	< 100	$< 10^{-7}$
4.	Telewizja	15 - 4000		$< 10^{-10}$
5.	Transfer plików	64 - 2000	> 1000	$< 10^{-8}$
6.	Fax grupy 4	64	< 200	$< 10^{-5}$

2 Standardy sieci WLAN ETSI

Opracowanie europejskiego standardu bezprzewodowych sieci lokalnych zostało zainicjowane przez ETSI w roku 1991 i trwało do 1996 r. Prace zakończyły się opracowaniem systemu HiPeRLAN typ 1 (ang. *High Performance Radio Local Area Network*). W roku 1997 rozszerzono zakres prac i opracowano rodzinę standardów dla sieci HIPERLAN zawierającą cztery typy sieci. Były to:

- typ 1 - bezprzewodowa sieć LAN o dużej szybkości przesyłanych danych;
- typ 2 - bezprzewodowy dostęp o małym zasięgu do sieci ATM;
- typ 3 - bezprzewodowy zdalny dostęp do sieci ATM;
- typ 4 - bezprzewodowe połączenie sieci ATM.

Sieci HIPERLAN typu od 2, 3, 4 są ukierunkowane na współpracę z sieciami zrealizowanymi w technologii ATM. W 1999 roku (ETSI, TR 101 031 v. 2.2.1) dokonano weryfikacji wcześniejszych ustaleń i wyróżniono następujące typy sieci HIPERLAN:

- typ 1 (bez zmiany) - bezprzewodowa sieć LAN o dużej szybkości przesyłanych danych;
- typ 2 (zmieniono) - bezprzewodowy dostęp o małym zasięgu do infrastruktury sieci IP, ATM, UMTS;
- HIPERACCES (uprzednio typ 3) - bezprzewodowy zdalny dostęp do infrastruktury sieci IP, ATM;
- HIPERLINK (uprzednio typ 4 - bezprzewodowe połączenie sieci szerokopasmowych.

Z przedstawionej charakterystyki wynika, że w sieci HIPERLAN typu 1 nie dokonano zmian natomiast w pozostałych typach sieci zmiany dotyczyły zarówno nazwy, wielkości parametrów łącza fizycznego oraz możliwości współdziałania bezprzewodowych sieci lokalnych z innymi infrastrukturami sieciowymi opartymi na technice ATM, IP oraz w sieci UMTS.

Tabela 2.1. Typy sieci HIPERLAN oraz HIPERACCESS i HIPERLINK

HIPERLAN TYP 1 (Bezprzewodowa LAN 8802)	**HIPERLAN TYP 2** (Bezprzewodowa IP, ATM i dostęp do UMTS dla małych odległości)	**HIPER-ACCESS** (Bezprzewodowa IP, ATM dla urządzeń wyniesionych)	**HIPERLINK** (Bezprzewodowe połączenia szerokopasmowe)	**HIPERMAN** (Bezprzewodowa IP (pętla lokalna)
DLC	**DLC**	**DLC**	**DLC**	**DLC**
PHY (5 GHz) **(19 Mbit/s)**	**PHY** (5 GHz) **(54 Mbit/s)**	**PHY** (zmienne pasmo) **(25Mbit/s)**	**PHY** (17 GHz) **(155 Mbit/s)**	**PHY** (< 11 GHz) **(25 Mbit/s)**

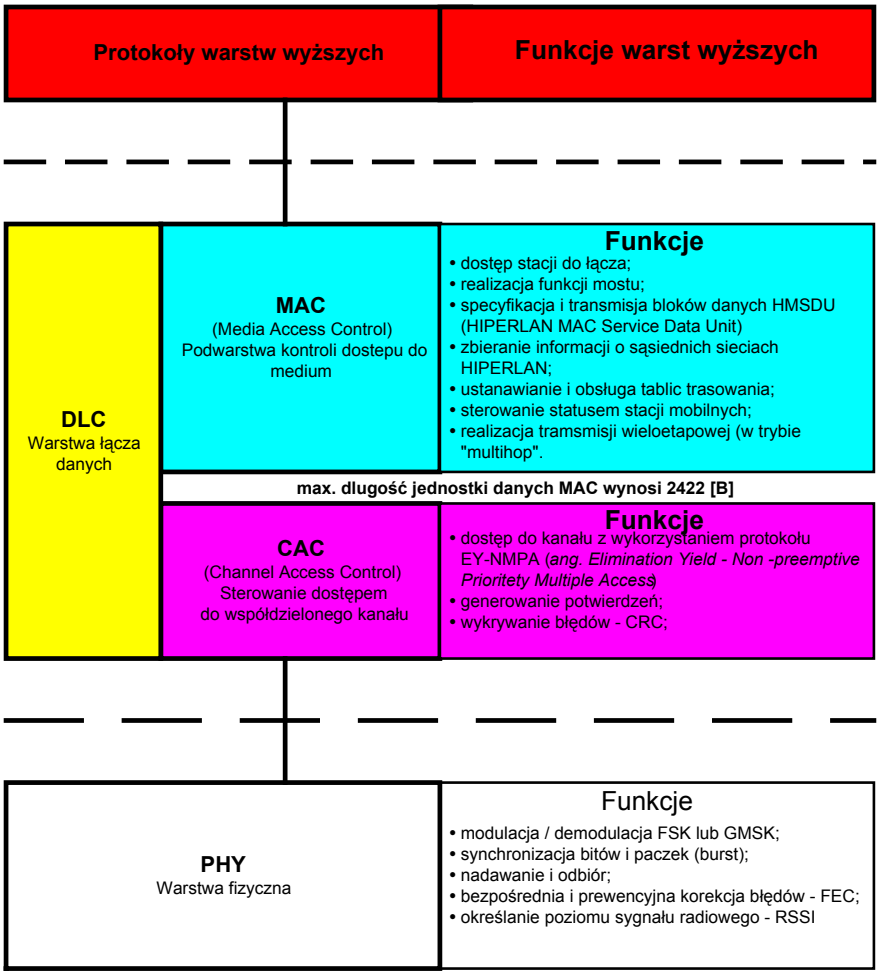
2.1 Bezprzewodowa sieć lokalna standardu HIPERLAN typu 1

Architektura sieci HIPERLAN (w tym także typu 1) została opracowana i jest zazwyczaj przedstawiana w postaci funkcjonalnego modelu warstwowego. W modelu wyróżniono trzy warstwy tj.

- Warstwa fizyczna - stanowi najniższy poziom oznaczany skrótem "PHY";
- Warstwa łącza danych - stanowi drugą w kolejności warstwę oznaczaną skrótem "DLC";
- Warstwy wyższe - stanowią najwyższy poziom modelu warstwowego i reprezentują podwarstwy zbieżności różnego typu sieci szkieletowych, z którymi sieć HIPERLAN współdziała.

W warstwie fizycznej są umiejscowione funkcje odpowiedzialne za realizację procesu nadawania i odbioru, w tym określanie poziomu sygnału radiowego, korekcję błędów, synchronizację bitową oraz realizację procesu modulacji (demodulacji).

Kolejna druga warstwa (łącza danych) została rozdzielona na dwie podwarstwy funkcjonalne. W pierwszej z nich - sterowania dostępem do medium - oznaczanej skrótem CAC (*ang. Channel Access Control*), umiejscowione są funkcje zapewniające dostęp do kanału, wykrywanie błędów oraz generowanie potwierdzeń. Druga z podwarstw - kontroli dostępu do medium - oznaczana skrótem MAC (*ang. Media Access Control*), należy do najbardziej złożonych podwarstw funkcjonalnych. Realizuje ona funkcje umożliwiające dostęp stacji do łącza, odpowiada za określanie i transmisję bloków danych, realizuje funkcje mostu, zbiera informacje o przyległych sieciach HIPERLAN oraz realizuje funkcje związane z ustanawianiem i obsługą tablic trasowania. W ramach funkcji własnych realizuje także transmisje wieloetapowe oraz steruje statusem stacji mobilnych. Opisane funkcje zostały przedstawione na rysunku 2.1.



Rys. 2.1. Model warstwowy sieci HIPERLAN 1

2.1.1 Warstwa fizyczna

W standardzie HIPERLAN zarezerwowano pasma 5.15 – 5.3 GHz oraz 17.1 – 17.3 GHz. Pasma te podzielono na kanały o szerokości 25 MHz z zastosowaniem obustronnych przedziałów ochronnych o szerokości 12.5 MHz. Transmisja ramek jest realizowana z dwiema różnymi prędkościami tj. małą prędkością bitową równą 1,4705875 Mbit/s (LBR - *ang. Low Bit Rate)* oraz dużą prędkością bitową równa 23,5294 Mbit/s (HBR - *ang. High Bit Rate*). Prędkość LBR jest wykorzystywana do przesyłania danych sterujących tj. potwierdzeń i nagłówków. Prędkość HBR jest używana tylko do wymiany ramek z danymi.

Na poziomie CAC używane są ramki danych, potwierdzeń i przydziału dodatkowych kanałów. Ramki potwierdzeń zawierają tylko część małej szybkości transmisji (LBR), która składa się z 35 bitów i zawiera:

- Preambułę (nagłówek);
- wskaźnik obecności części związanej z dużą szybkością (HBR);
- skrócony adres docelowy;
- wskaźnik długości bloku.

Adres docelowy i wskaźnik długości bloku są zabezpieczone 4 bitową sumą CRC.

2.1.2 Wybrane parametry przykładowych sieci HIPERLAN

W standardzie sieci lokalnej HIPERLAN typ 1 zdefiniowano wirtualną podsieć radiową, która może być przyłączona do sieci przewodowej znajdującej się wewnątrz obiektu. Sieć pracuje w paśmie od 5,15 do 5,3 GHz a moce nadajników zawierają się w przedziale od 10 mW do 1 W co odpowiada zasięgowi od 10 do 100 metrów. W tabeli 2.2 przedstawiono charakterystyczne parametry sieci dla sieci i urządzeń sieci HIPERLAN typu 1.

Tabela 2.2. Charakterystyczne parametry sieci HIPERLAN typu 1.

LP	Rodzaj parametru	Wielkości
1.	Częstotliwość pracy	5,15 - 5,3 GHz; 17,1- 17,3 GHz
2.	Moc nadawania	0,1 – 1 W; 0,1 W
3.	Czułość odbiornika	50, 60, 70 [dBm]
4.	Kanały	5 (z dostępem FDMA)
5.	Szerokość kanału	23,5294 MHz
6.	Maksymalna prędkość liniowa	1,4 m/s
7.	Funkcje	- potwierdzanie, - wykrywanie błędów CRC 32 bit; - korekcja błędów FEC (31, 26,3 - typ kodowania BCH; - połączenie typu punkt - punkt - zmienna długość pakietu; - ograniczony czas dla transferowanych pakietów
8.	Rodzaje przepływność i rodzaj modulacji: HBR (*High Bit Rate*) LBR (*Low Bit Rate*)	23,5294 Mbit/s - GMSK (*ang. Gaussian Minimum Shift Keying*) 1,47060 Mbit/s -FSK

W ramach standardu nie jest wyspecyfikowany mechanizm przekazywania stacji (*handover*).

W sieciach HIPERLAN jest możliwa realizacja następujących aplikacji:

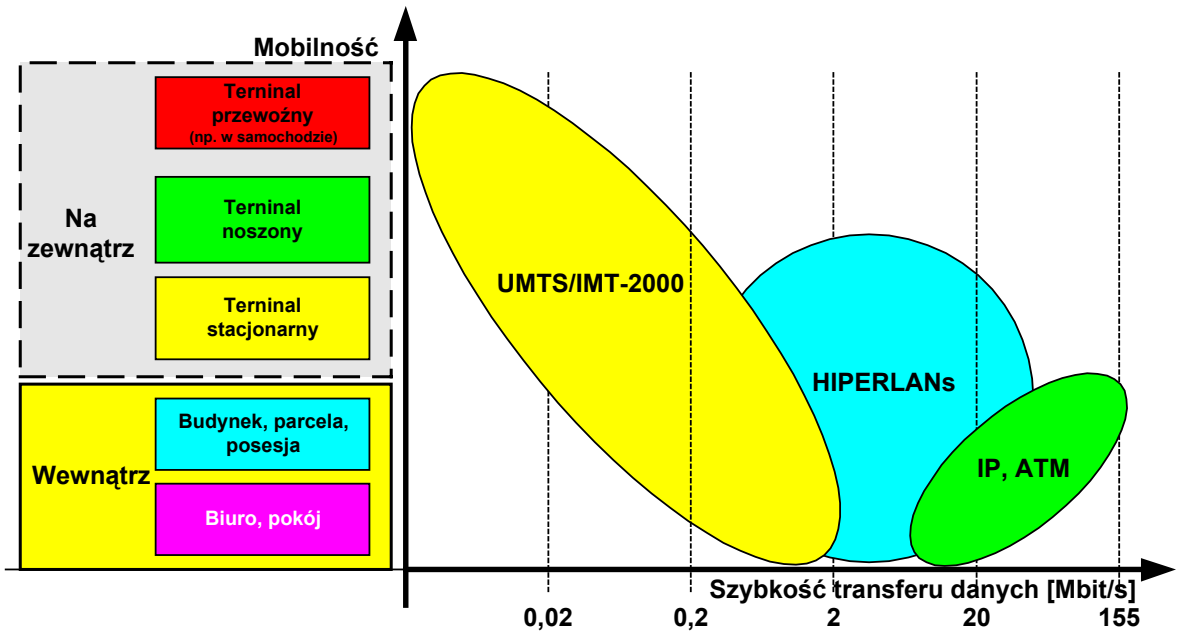
- telekonferencja;
- video;
- transmisja danych medycznych np. zdjęcia kardiogramy;
- eksploatacyjne dane związane z funkcjonowaniem stacji kolejowych, portów w tym lotniczych;
- zdalne sterowanie robotami np. w rejonach czy strefach niebezpiecznych skażeń.

W sieci HIPERLAN typu 1 realizowane są trzy typy sygnałów nadawczo/odbiorczych. W tabeli 2.3 wyszczególniono możliwe kombinacje klas nadajników i odbiorników.

Tabela 2.3. Kombinacje klas nadajników i odbiorników w sieci HIPERLAN typu 1

Nadajnik / **Odbiornik**	Klasa "A" (+10 [dBm])	Klasa "B" (+20 [dBm])	Klasa "C" (+30 [dBm])
Klasa "A" (czułość -50 [dBm])	dozwolona	Nie dozwolona	Nie dozwolona
Klasa "B" (czułość -60 [dBm])	dozwolona	dozwolona	Nie dozwolona
Klasa "C"(czułość -70 [dBm])	dozwolona	dozwolona	dozwolona

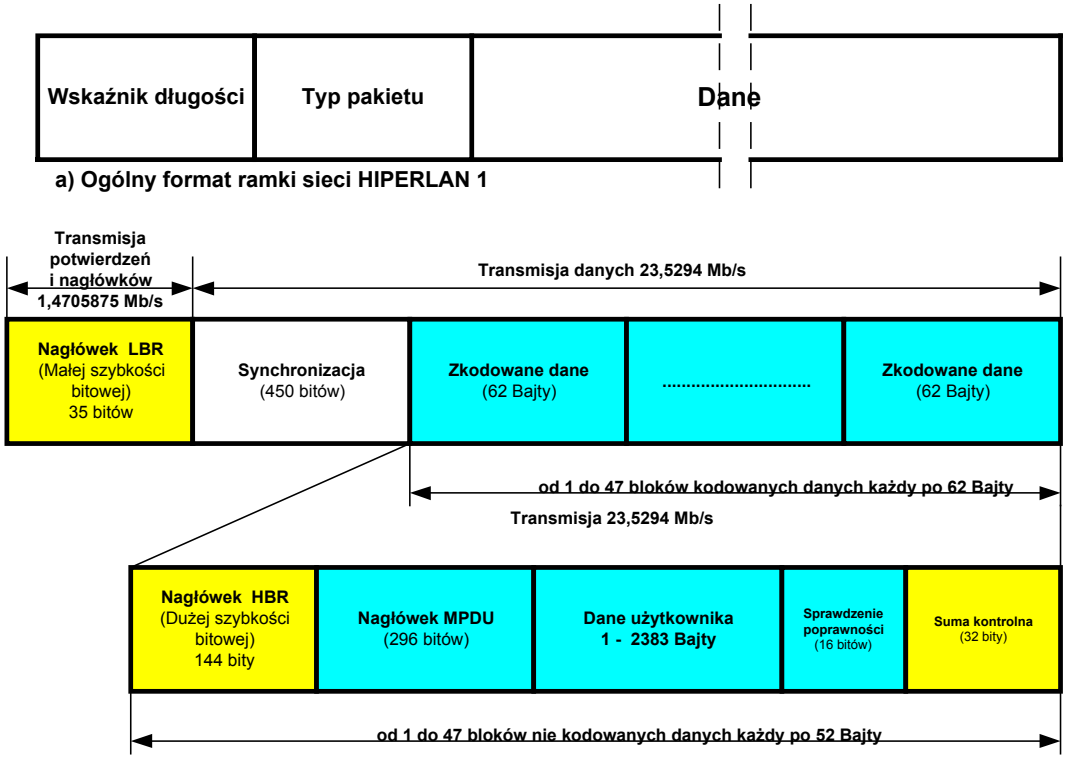
Uwaga: czułość jest definiowana jako minimalny poziom mocy pozwalający na uzyskanie parametru PER (ang. *Packet Error Rate*) na poziomie 0,01 dla pakietów o długości 4160 bitów.



Rys. 2.2. Związki systemu HIPERLAN z typami sieci szkieletowych

Część ramki dużej szybkości (HBR) zawiera następujące dane:

- wskaźnik obecności danych;
- wskaźnik długości bloku;
- wskaźnik długości pola rozszerzenia;
- identyfikator sieci HIPERLAN;
- adres źródła i przeznaczenia;
- pole danych;
- pole dodatkowe.



b) Dokladny format ramki danych dla sieci HIPERLAN typu 1

Rys. 2.3. Format ramki danych sieci HIPERLAN1

Pole HBR jest zabezpieczane przez 32 bitowe pole CRC. W omawianym standardzie na poziomie CAC stosowany jest protokół niewymuszonego, priorytetowego dostępu do łącza (EY-NMPA)[2], który przewiduje trzy procedury dostępu do kanału:

- wolnego;
- zajętego z synchronizowaniem się stacji z końcem cyklu zajętości kanału;
- w przypadku tzw. "ukrytej eliminacji" (ang. *Channel Access in Hidden Elimination Condition*).

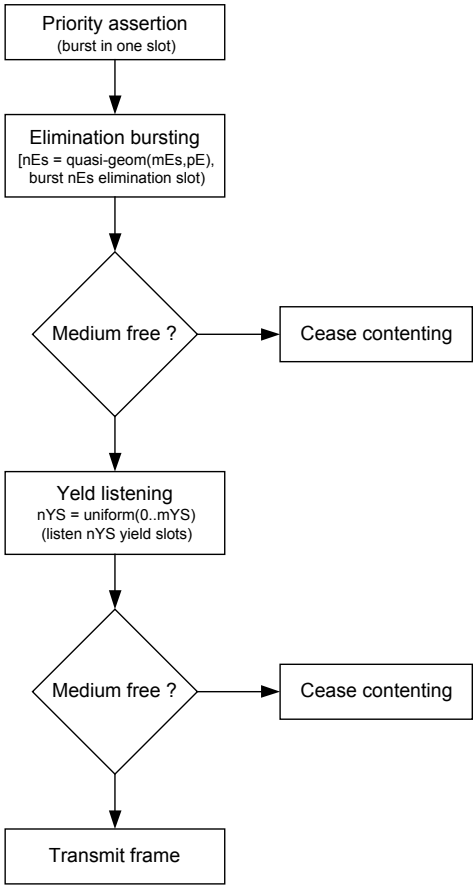
Dostęp do kanału wolnego występuje, gdy stacja nie obserwuje aktywność we wspólnym kanale przez okres odpowiadający czasowi transmisji, co najmniej 1800 bitów z dużą przepływnością (HBR). Wówczas kanał traktuje się jako wolny i można rozpoczynać transmisję bez żadnych dodatkowych procedur. Czas odpowiadający 1800 bitom HBR może być wydłużony do trzech dodatkowych okresów, o długości 200 bitów każdy

W wypadku stwierdzenia, że w kanale jest realizowane przygotowanie do transmisji lub transmisja jest realizowana (kanał jest zajęty) stacja przeprowadza synchronizacje własnych procedur z końcem cyklu transmisyjnego. Cykl taki składa się z następujących faz:

- zgłaszania priorytetów i wyłaniania stacji (lub kilku stacji) o najwyższym priorytecie;
- rywalizacji z okresem eliminacji i okresem rozstrzygania oraz wyłaniania jednej lub kilku stacji, które "przeżyły" w tym procesie;
- transmisji.

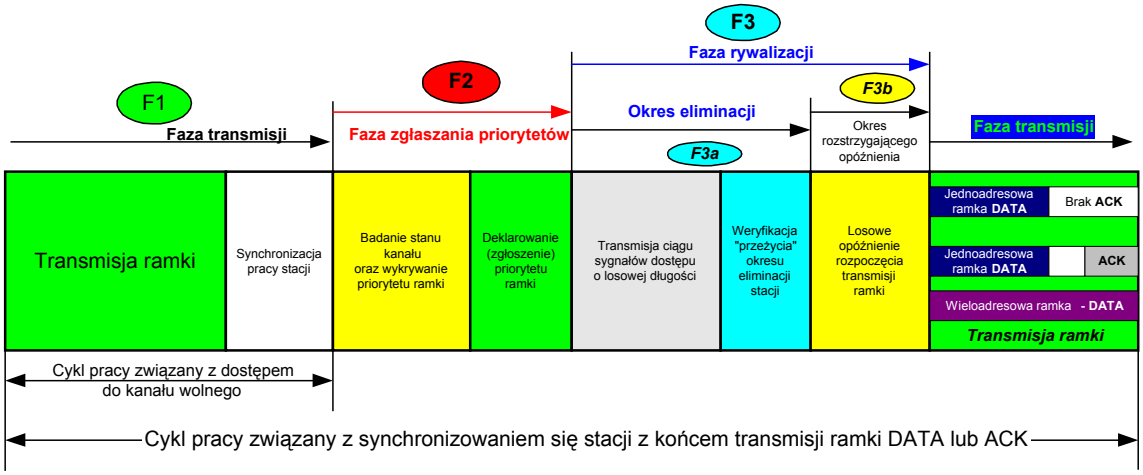
Jak wspomniano wcześniej w podwarstwie CAC stosowany jest protokół oparty na algorytmie EY - NPMA. Działanie standardowego algorytmu EY - NPMA w sieci HIPRERLAN zilustrowano na rysunku 2.4.

[2] *ang. Elimination Yield - Non preemptive Priority Multiple Access*



Rys. 2.4. Standardowy algorytm protokołu niewymuszonego, priorytetowego dostępu do medium

Procedura EY - NPMA zapewnia hierarchiczną niezależność dostępu do kanału ramkom o priorytetach zdefiniowanych w podwarstwie HIPERLAN MAC. Procedura protokołu stanowi kombinację metod CSMA z algorytmami eliminacji i rozwiązywania powstających konfliktów. Podział cyklu transmisyjnego protokołu EY-NPMA (oznaczany także jako NPMA) zobrazowano na rys. 2.5.



Rys. 2.5. Cykl transmisyjny protokołu EY-NPMA sieci HIPERLAN typu 1

Po zakończeniu cyklu transmisji ramki (F1 na rys. 2.5) następuje faza wyłaniania ramek o najwyższym priorytecie (F2). Przyjmuje się istnienie określonej liczby priorytetów oznaczonych od 0 do pewnej wartości[3] pomniejszonej o jeden, gdzie 0 oznacza najwyższy priorytet dostępu.

[3] *zakładając jednoczesną pracę 256 stacji rozlokowanych na obszarze o promieniu 50 [m] standard HIPERLAM 1 CAC proponuje wartość równą 5 przy gwarancji częstość kolizji ramek na poziomie poniżej 3,5 [%]*

Priorytet dostępu zależy od ważności informacji i wartości tzw. znormalizowanego czasu życia ramki - NRL. W trakcie rozpoczęcia się kolejnego cyklu oś czasu dzielona jest na szczeliny czasowe, które nazywane są szczelinami priorytetyzacji (168 bitów HBR). Wyłanianie najwyższego priorytetu ramek jest realizowany przez detekcję kanału oraz deklarowanie priorytetów ramek.

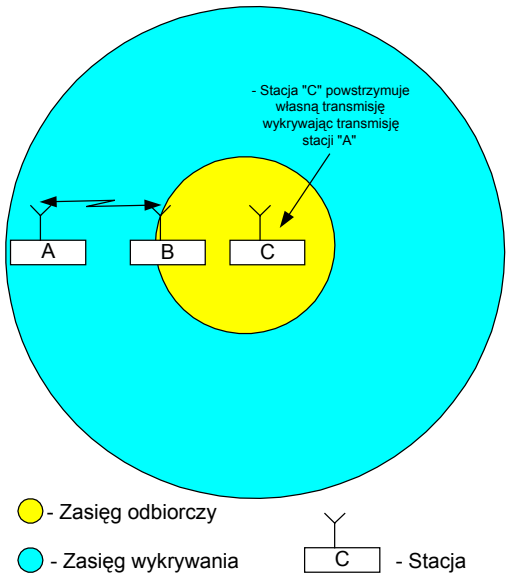
Przed nadaniem ramki o priorytecie np. ***n*** stacja bada stan kanału przez ***n*** pierwszych szczelin priorytetyzacji (n x 168 bit). Jeżeli w tym czasie nie stwierdzi aktywności w kanale, stacja generuje ciąg sygnałów deklarując priorytet ramki. Inne stacje po stwierdzeniu, że mają do przesłania ramki o niższym priorytecie niż ***n*** rezygnują z ubiegania się o dostęp do medium w danym cyklu. Wynika stąd, że przynajmniej jedna z rywalizujących stacji zawsze pozostaje aktywna.

Faza rywalizacji o dostęp do kanału (F3 na rys. 2.5.) zawiera dwa okresy tj. eliminacji stacji i rozstrzygnięcia konfliktu. Zakończenie fazy deklarowania priorytetów powoduje kolejną dyskretyzację osi czasu powodując podział kanału na tzw. szczeliny eliminacji. Stacje mające do przesłania ramki o najwyższym priorytecie (wyłonione w poprzedniej fazie) przesyłają ciągi sygnałów eliminacji będących wielokrotnością szczeliny eliminacji. Długość ciągu eliminacji może zmieniać się od 0 do 12 szczelin eliminacji zgodnie z rozkładem geometrycznym.

Stacja po przesłaniu sygnału eliminacji o długości od 0 do określonej wartości szczelin eliminacji przechodzi w stan nasłuchu przez dany przedział czasowy (256 bitów HBR). Jeżeli po zakończeniu transmisji ciągu stwierdza inną transmisję, to rezygnuje z ubiegania się o dostęp do medium w danym cyklu. Stacja "przeżywa" eliminacje tylko wtedy, gdy po zakończeniu transmisji ciągu eliminacji stwierdza, że kanał jest wolny. Czas trwania oczekiwania jest więc wyznaczany przez czas trwania najdłuższego ciągu eliminacji.

Ostatnia część okresu rywalizacji o dostęp do medium (F3b na rys. 2.5.) jest realizowana poprzez kolejną dyskretyzację chwil dostępu do kanału i podział czasu pracy kanału na szczeliny o określonej długości. Stacje, które zwycięsko zakończyły okres rywalizacji mogą rozpocząć transmisję z opóźnieniem od 0 do określonej wielokrotności długości szczeliny wcześniej opisanego podziału czasu pracy kanału (np. 9). Opóźnienie w transmisji ma charakter losowy i jest opisane rozkładem równomiernym.

Dostęp do kanału w przypadku tzw. "ukrytej eliminacji" jest realizowany wtedy, kiedy nie wszystkie stacje się "słyszą". Sytuacja taka może wystąpić wtedy, gdy stacja przegrywa rywalizację w dowolnej fazie, ale nie wykrywa transmisji. Wtedy stacja zakłada, że proces rywalizacji został wygrany przez stację znajdującą się poza jej zasięgiem. Zaistniała sytuacja powoduje, że stacja przechodzi w stan "ukrytej eliminacji" trwający 500 ms. Opisana sytuacja została przedstawiona graficznie na rysunku 2.6.



Rys. 2.6. Graficzne zobrazowanie eliminacji "ukrytej stacji" - protokół EY-NPMA

W stanie "ukrytej eliminacji", sterowanie dostępem stacji do kanału realizują dwa liczniki. Pierwszy (500 ms), odmierzający czas pozostawania w tym stanie i drugi odmierzający opóźnienia ewentualnych prób dostępu wynoszący od 1 do 5 ms.

Opóźnianie prób dostępu przez stację oznacza, że nie uczestniczy ona w rywalizacji o prawo transmisji w każdym cyklu transmisyjnym, lecz włącza się do rywalizacji, co pewien losowy przedział czasu. W ten sposób zostaje ograniczony niekorzystny wpływ efektu stacji "ukrytych" na jakość pracy sieci, lecz wydłuża się opóźnienie transmisji ramek.

Faza transmisji charakteryzuje się tym, że obiekty mogą podejmować następujące działania:

- transmitowanie ramek jednoadresowych i towarzyszące im transmisje potwierdzeń;
- transmitowanie ramek wieloadresowych (bez transmisji potwierdzeń);
- transmisję ramek z informacją o dostępności kanałów 3 i 4.

Tabela 2.4. Porównanie parametrów standardów IEEE 802.11 oraz HIPERLAN

Lp.	Parametry	HIPERLAN	IEEE 802.11 DSSS	IEEE 802.11 FHSS
1.	Czas oczekiwania przed nadaniem pakietu	85 µs	50 µs	128 µs
2.	Przerwa międzyramkowa przed nadaniem potwierdzenia	21,8 µs	10 µs	28 µs
3.	Dodatkowe informacje podczas przekazu z małą prędkością	35 bit/1,47 Mb/s	128 bit/1 Mb/s	192/1 Mb/s
4.	Maksymalna efektywność przepływności w bezprzewodowej sieci dla transmisji jednego pakietu	78,4%	97,7 % /2 Mb/s 98,8 % /1 Mb/s	99,2 % /2 Mb/s 99,6 % /1 Mb/s
5.	Efektywność przepływności w bezprzewodowej sieci dla transmisji jednego 1518 Bajtowego pakietu Ethernet	74,1%	96,9 % /2 Mb/s 98,4 % /1 Mb/s	97,9 % /2 Mb/s 99,0 % /1 Mb/s
6.	Czas transmisji dla jednego pakietu Ethernet o dł. 1518 Bajtów	696,4 µs	6,264 µs /2 Mb/s 12,336 µs /1 Mb/s	6,200 µs /2 Mb/s 12,272 µs /1 Mb/s
7.	Czas transmisji potwierdzenia	15,6 µs	248 µs /2 Mb/s 304 µs /1 Mb/s	184 µs /2 Mb/s 240 µs /1 Mb/s

HIPERLAN zapewnia QoS typu *"best effort"* z kontrolą czasu życia pakietu. Zastosowano liniową reprezentację porównywania pięciu poziomów priorytetów. Priorytet pakietu jest funkcją definiowaną przez użytkownika i "pozostałości sieciowej". Priorytety i czas życia pakietów w HIPERLAN 1 został przedstawiony w tabeli 2.5.

Tabela 2.5. Priorytety i czas życia pakietów w HIPERLAN 1

Znormalizowany czas życia pakietu - NRL (Normalized Residual Liftime)	Wysoki priorytet	Niski priorytet
10 ms > NRL	0 (najwyższy)	1
20 ms >NRL ≥ 10 ms	1	2
40 ms >NRL≥ 20 ms	2	3
80 ms >NRL ≥ 40 ms	3	4
NRL ≥ 80 ms	4 (najniższy)	4

Podczas oczekiwania pakietu w kolejce do transmisji jego dopuszczalny czas życia będzie malał. Węzeł może zadecydować o zmianie priorytetu obsługi pakietu stosownie do tego, jaki pozostał czas życia pakietu. Pakiety, których czas życia wynosi zero są kasowane. Dla obsługi pakietów o tym samym priorytecie obowiązuje strategia obsługi "pierwszy przybył pierwszy obsłużony - FCFS (ang. *first - come -first - served*).

Sieci HIPERLAN typu 1 na poziomie protokołu podwarstwy MAC dokłada maksymalnych starań (ang. *best effort*), aby spełnić warunki w zakresie dopuszczalnego opóźnienia dla ruchu izochronicznego (np. videotelefonia) oraz odpowiedniego poziomu integralności dla ruchu typu asynchronicznego (np. transfer plików). Ponieważ dane mogą być transferowane do miejsca przeznaczenia przez więcej niż jeden węzeł transferowy, dlatego odwzorowanie priorytetów uwzględnia liczbę kolejnych kroków w czasie transportu ramki.

2.2 Bezprzewodowa sieć HIPERLAN typu 2

2.2.1 Model odniesienia i architektura systemu HIPERLAN typu 2

HIPERLAN typu 2 (HIPERLAN2) zapewnia bezprzewodowy dostęp do usług w niewielkiej odległości od punktu dostępowego sieci szkieletowych (IP, ATM, UMTS). Obszar działania HIPERLAN2 jest ograniczone przez zasięg systemu bezprzewodowego, zaś funkcje sieci tego typu podzielono na następujące kategorie:

- Warstwa fizyczna - zapewnia kolejność transferu bitów pomiędzy parą węzłów, lecz np. dla stron wykorzystujących protokół TCP/IP takiej własności nie posiada.
- Warstwa sieciowa - realizuje procedury, które pozwalają na transport danych w trybie bezpołączeniowym miedzy wieloma sieciami (np. routing, segmentacja, itp.).
- Warstwa transportowa - zapewnia wymianę danych między dwoma hostami zarówno w trybie połączeniowym jak i bezpołączeniowym, włączając także sterowanie przepływem, obsługę błędów itp.
- Warstwa aplikacji – obejmuje protokoły umożliwiające dzielenie zasobów zdalnego dostępu, transfer danych itp.

Odpowiednio system ATM zawiera:

- Warstwę fizyczną ATM (transport bitów);
- Warstwę ATM (tworzenie komórek, komutacja);
- Warstwy AAL w tym warstwę umożliwiającą zestawianie połączeń (SAAL) oraz inne warstwy AAL odpowiednio do bazowych klas usług ATM.

Sieć HIPERLAN2 umożliwia realizację następujących usług:

- Zestawianie połączeń z gwarantowaną jakością w połączeniu z siecią szkieletową;
- Obsługę połączeń przychodzących i wychodzących, transfer danych i QoS;
- Udostępnianie zasobów do realizacji wymienionych usług, w tym *handover* miedzy punktami dostępowymi i siecią szkieletową;
- Zarządzanie zasobami energetycznymi (zasilania);
- Dynamiczną alokację częstotliwości i zasobów do tworzenia kanałów radiowych;
- Realizacja funkcjonalnej sieci doraźnej (*ad-hoc*).

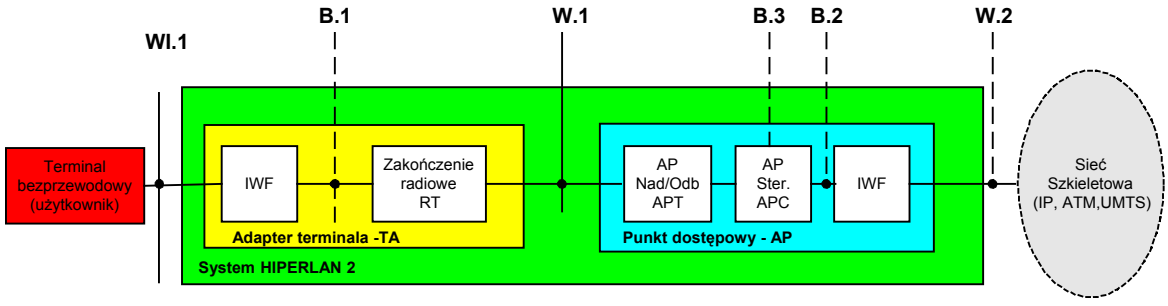
2.2.2 Funkcjonalny model odniesienia sieci HIPERLAN2

Sieć HIPERLAN2 zawiera dwa główne elementy funkcjonalne tj. punkt dostępowy do sieci szkieletowej określonego typu oraz adapter terminala użytkownika. W punkcie dostępowym wyróżniono trzy wewnętrzne elementy funkcjonalne. Są to: element współpracy funkcji międzysieciowych (IWF), kontroler (sterownik) punktu dostępowego (APC) oraz nadajnik/odbiornik punktu dostępowego (APT). Element IWF występuje także w adapterze terminali (TA), odpowiedzialnym za translację wewnętrznych interfejsów HIPERLAN2. Występując w składzie AP dokonuje translacji wewnętrznego interfejsu sieci HIPERLAN2 (B.2) na specyficzny interfejs zewnętrznej sieci szkieletowej (W.2).

Kontroler (sterownik) punktu dostępowego (APC) realizuje specyficzne funkcje interfejsu z siecią szkieletową poprzez element IWF, który jest zgodny z odpowiednim standardem (np. sieci IP). APC zapewnia mechanizmy ułatwiające realizację funkcji "handover" pomiędzy punktami dostępowymi i steruje routingiem ruchu poprzez sieć HIPERLAN2.

Nadajnik/odbiornik punktu dostępowego (APT) rozdziela zasoby w taki sposób, aby zapewnić wymaganą przepływność dla usług z obszaru dostępnego w szerokopasmowych dostępowych punktach radiowych sieci (BRAN). Komunikuje się także z zakończeniem radiowym adaptera terminala poprzez interfejs (W.1).

W adapterze terminala użytkownika wyróżnione zostały dwa elementy funkcjonalne tj. zakończenie radiowe (RT) oraz element współpracy funkcji międzysieciowych (IWF). Zakończenie radiowe (RT) stanowi radiową część adaptera terminala, natomiast funkcja współpracy międzysieciowej IWF dokonuje translacji wewnętrznego interfejsu TA (B.1) na wyższe warstwy protokołu terminala bezprzewodowego. Wymienione elementy funkcjonalne przedstawiono na rysunku 2.7.



Rys. 2.7. Funkcjonalny model odniesienia sieci HIPERLAN2

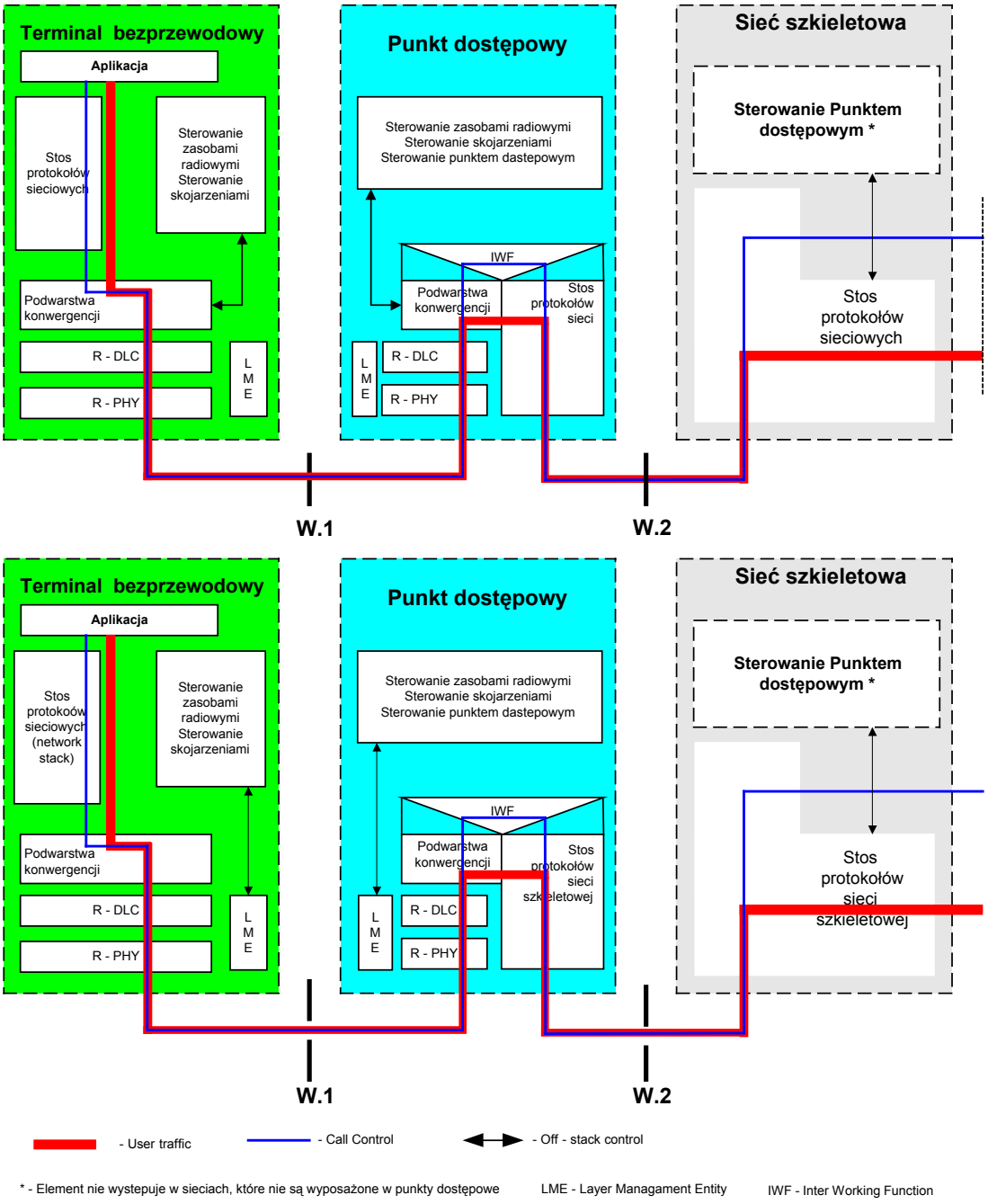
Tworzące system elementy funkcjonalne rozdzielone są punktami odniesienia, których nazwy oraz charakterystykę przedstawiono w tabeli 2.6.

Tabela 2.6. Wykaz punktów odniesienia (interfejsów) w modelu sieci HIPERLAN2

Lp.	Punkt odniesienia	Opis
1.	**WI.1**	Interfejs terminala bezprzewodowego (wewnętrzny lub standardowy), który zależy od rodzaju współpracującej sieci szkieletowej.
2.	**B.1**	Interfejs usług, zdefiniowany jako zbiór abstrakcyjnych jednostek usługowych i ich parametrów dla stosu protokołów interfejsu bezprzewodowego (radiowego) w płaszczyznach użytkownika, sterowania i zarządzania sieci HIPERLAN2. Przyjmuje się, że będzie to wspólny interfejs dla systemu HIPERLAN2 i systemów HIPERACCESS, określający zasady współpracy na wspólnym interfejsie bezprzewodowym. Interfejs ten nie jest wymagany w rzeczywistych implementacjach sprzętowych, lecz jego specyfikacja musi być weryfikowana przy testowaniu funkcjonalności.
3.	**W.1**	Definiuje interfejs radiowy między nadajnikiem/ odbiornikiem punktu dostępowego (APT) i zakończeniem radiowym (RT) adaptera terminala. Jest to standaryzowany interfejs bezprzewodowy zapewniający współdziałanie różnych systemów.
4.	**B.2**	Podobnie jak interfejs usług (B.1), został zdefiniowany jako zbiór abstrakcyjnych jednostek usługowych i ich parametrów dla stosu protokołów interfejsu bezprzewodowego (radiowego) w płaszczyznach użytkownika, sterowania i zarządzania sieci HIPERLAN2. Przyjmuje się, że będzie to wspólny interfejs dla systemu HIPERLAN2 i systemów HIPERACCESS, określający zasady współpracy systemów we wspólnym interfejsie bezprzewodowym. Interfejs ten nie jest wymagany w rzeczywistych implementacjach sprzętowych, lecz jego specyfikacja stanowi podstawę przy testowaniu funkcjonalności. ***Uwaga:*** *W skład punkt dostępowego AP może wchodzić jeden lub kilka elementów nadawczo/odbiorczych (APT) przyłączonych do pojedynczego kontrolera punktu dostępowego (APC). Interfejs miedzy tymi elementami nie musi być wyróżniany i nie jest przedmiotem standaryzacji.*
5.	**W.2**	Standardowy interfejs zapewniający sprzęg z odpowiednim typem sieci szkieletowej. Komplet interfejsów może być ze standaryzowany w ramach projektu BRAN.
6.	**B.3**	Jest interfejsem, w którym wyspecyfikowane są mechanizmy zapewniające komunikację z elementami systemu zarządzania, specyficzny dla zarządzania sieciowym punktem dostępu radiowego.

2.2.3 Warstwowy model protokołów sieci HIPERLAN2

W architekturze protokołów sieci HIPERLAN2, przedstawionej na rysunku 2.8, występują (podobnie jak w wcześniej przedstawionym modelu funkcjonalnym) trzy elementy funkcjonalne tj. terminal bezprzewodowy, punkt dostępowy do sieci szkieletowej oraz element sieci szkieletowej. We wszystkich elementach funkcjonalnych umiejscowiono protokoły służące do transportu danych użytkownika oraz protokoły związane z sygnalizacją oraz zarządzaniem zapewniające współpracę z siecią szkieletową przy wykorzystaniu środowiska zarówno bezprzewodowego jak i przewodowego.



Rys. 2.8. Architektura warstwowa protokołów sieci HIPERLAN2

W oparciu o warstwowy model OSI, wewnątrz przedstawionych elementów funkcjonalnych, zaznaczono nazwy zestawów protokołów oraz ścieżkę przepływu wiadomości związanych z zestawianiem i sterowaniem połączeniem (kolor niebieski) jak i ścieżkę przesyłanych wiadomości użytkownika (kolor czerwony). Czarna linia zakończona strzałkami obrazuje interfejsy od strony stosu protokołów, które pozwalają użytkownikowi dostarczać funkcji do sterowania warstwą łącza danych (DLC) takich jak zestawianie połączenia lub jego rozłączanie. W zależności od funkcji elementu w systemie poszczególne elementy funkcjonalne posiadają zróżnicowaną warstwową architekturę protokołów.

Terminal bezprzewodowy komunikujący się z siecią szkieletową poprzez punkt dostępowy realizuje protokoły:

- warstwy fizycznej umożliwiające komunikację z wykorzystaniem wolnej przestrzeni przy pomocy fal radiowych (R-PHY);
- warstwy łącza danych do współpracy z medium bezprzewodowym (R-DLC);

- warstwy konwergencji (segmentacji lub składania wiadomości) umożliwiające dostęp do zasobów sieci szkieletowej (IP, ATM, UMTS);
- stosu protokołów warstw wyższych umożliwiających realizacje różnych aplikacji, których protokoły umiejscowiono w warstwie aplikacyjnej;
- jednostek zarządzania warstwą (LME) na poziomie warstwy fizycznej i łącza danych oraz stosu protokołów związanych ze sterowaniem zasobami radiowymi, skojarzeniami poszczególnych procesów aplikacyjnych itp.

Dostępowy punkt sieci szkieletowej (AP), na poziomie warstw niższych posiada od strony współpracującego z nim poprzez interfejs W.1 terminala kompatybilny zestaw protokołów. Dodatkowo, od strony współpracującej z AP poprzez interfejs W.2 sieci szkieletowej posiada zestaw protokołów odpowiedni do typu współpracującego systemu. Na poziomie warstw wyższych AP nie posiada protokołów odpowiedzialnych za realizację procesów aplikacyjnych użytkownika, a jedynie protokoły płaszczyzny sterowania.

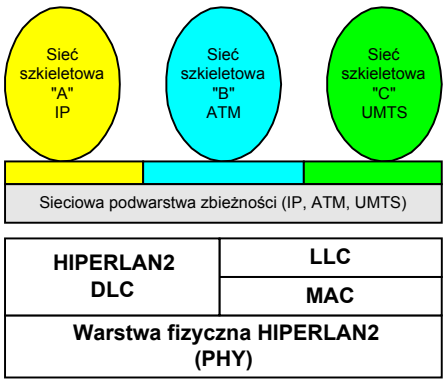
Omawiany punkt dostępu pełni rolę multipleksera, który zapewnia mobilność terminali bezprzewodowych obsługiwanych w danej podsieci. Dostarcza także niezbędnych informacji dla sieci szkieletowej, tak aby możliwe było zapewnienie wymaganej mobilności terminali.

W radiowej warstwie DLC umiejscowione są mechanizmy realizujące określoną politykę zapewnienia jakości obsługi użytkownika, do których należy zaliczyć jakość kanału, liczba terminali i odpowiedni podział zasobów fizycznych oraz ich dostępność dla innych podsieci. Z konieczności zapewniania poziomu jakości obsługi przez warstwę DLC wynika także potrzeba implementowania różnorodnych mechanizmów pomocniczych w rodzaju FEC, ARQ itp.

W warstwie DLC umiejscowione są jednostki podsystemu zarządzania LME[4], których zasadniczym zadaniem jest przekazywanie informacji związanych z parametrami kontraktu ruchowego i realizacją wymaganych uzgodnień pomiędzy DLC i funkcjami sterowania połączeniami umiejscowionymi w wyższych warstwach architektury.

Podwarstwa konwergencji współpracując z DLC i poprzez funkcje IWF z siecią szkieletową realizuje wiele funkcji. Głównie jest odpowiedzialna za segmentację i składanie ramek oraz przekazywanie informacji pomiędzy protokołami, znajdującymi się na różnych poziomach modelu warstwowego, wykorzystywanymi przez funkcje zarządzania oraz mechanizmy służące do zapewnienia jakości obsługi (QoS).

Współpracujący element sieci szkieletowej posiada stos protokołów odpowiedni dla rodzaju zastosowanej techniki transferowania pakietów.



Rys. 2.9. Współpraca międzysieciowa HIPERLAN2 z różnymi rodzajami sieci szkieletowych

Sieci realizowane w standardzie HIPERLAN2 posiadają duże znaczenie, szczególnie w perspektywie upowszechnienia systemu UMTS.

[4] *ang. Layer Management Entity*

2.3 System HIPERACCES

2.3.1 Wprowadzenie

Tworzenie i standaryzacja systemu HIPERACCES (*ang. High PErformance Radio ACCESS*) jest odpowiedzią na wzrastające zapotrzebowanie na cyfrowe i szerokopasmowe usługi telekomunikacyjne w środowiskach:

- indywidualnych użytkowników domowych;
- właścicieli prowadzących małej i średniej wielkości przedsiębiorstwa - SME.[5];
- infrastruktur mobilnych wymagających realizacji usług telekomunikacyjnych związanych ze spędzeniem wolnego czasu, rekreacją i rozrywką.

Standaryzacja wspomnianego systemu została podjęta przez ETSI. Do kluczowych zagadnień standaryzacji zalicza się określenie wymagań funkcjonalnych, specyfikacje techniczne dla pojedynczo współpracujących systemów oraz ich rozwój. W tym zakresie mieści się także podejmowanie działań dla obniżania kosztów użytkowania i ograniczanie liczby różnorodnych opcji systemu. Przyjmuje się jednak, że opracowany standard może być kompromisem kilku opcji wynikających lub uwzględniających różne zakresy częstotliwości oraz różnych schematów podziału kanałów. W chwili obecnej standaryzacja obejmuje następujące obszary:

- Ogólnej charakterystyki systemu;
- Wymagań i architektury;
- Warstwy fizycznej (PHY);
- Współdziałania podwarstw w ramach warstwy sterowania łączem danych - DLC (*ang. Data Link Control);*
- Podwarstwy konwergencji i współpracy z systemami opartymi na technice IP i ATM;
- Części utrzymania i zarządzania systemem (OAM);
- Testowania zgodności.

HIPERACCES wykorzystuje system radiowy w realizacji następujących zasadniczych zadań:

- realizacji usług głosowych i transmisji danych;
- łączenia indywidualnych użytkowników i sieci, oferując pasmo dla wymaganych szybkości transmisji danych w trybie doraźnym lub „na życzenie”;

Przykłady podstawowych wymagań potencjalnych użytkowników systemu oraz możliwe do określenia szybkość transmisji danych dla sektora komercyjnego przedstawiono w poniższych tabelach.

[5] *ang. Small to medium sized enterprises*

Tabela 2.3.1 Zasadnicze usługi, typy użytkowników oraz istotne własności systemu

Wymagane usługi	Typ użytkownika	Własności HIPERACCES
Dostęp do Internetu	Mieszkaniowy/SME	Pojemność, elastyczność i efektywność
Usługi czasu rzeczywistego	Mieszkaniowy/SME	Pojemność, elastyczność i efektywność
Gry komputerowe (pobieranie zbiorów i interaktywne sesje)	Mieszkaniowy	Pojemność, elastyczność i efektywność
Wideokonferencje	Mieszkaniowy /SME	Pojemność, elastyczność i efektywność
Video na życzenie/prawie VoD	Mieszkaniowy/SME	Pojemność, elastyczność i efektywność
Dostęp do sieci LAN	Mieszkaniowy/SME	Pojemność, elastyczność i efektywność
Równoczesne wykorzystanie przez wielu użytkowników	Mieszkaniowy/SME	Pasmo na żądanie i obsługa zakończeń usługowych (np. E1, n x 64 kbit/s)
Dostęp do sieci Internet	SME	Pojemność, elastyczność i efektywność
CES	SME	Pojemność, elastyczność i efektywność
Telepraca	Mieszkaniowy/SME	Pojemność, elastyczność i efektywność
Usługi archiwizacji i magazynowania danych	Mieszkaniowy/SME	Realizacja usług POTS i ISDN, fax. (np. w paśmie akustycznym z wykorzystaniem modemu)

Tabela 2.3.2.: Przykłady średniej i maksymalnej szybkości transmisji dla sektora komercyjnego

Aplikacje	Średnia szybkość	Maksymalna szybkość
Kodowana mowa o niewielkiej szybkości bitowej	5,3 kbit/s	32 kbit] /s
POTS/ ISDN	64 kbit/s	144 kbit/s
Internet w mieszkaniu/gry komputerowe/ rozrywka	Patrz uwaga	2 - 25 Mbit/s
Użyteczność/bezpieczeństwo publiczne	Patrz uwaga	2 Mbit/s
Komercyjny handel elektroniczny	Patrz uwaga	2 - 8 Mbit/s
Teleedukacja/ telemedycyna	Patrz uwaga	2 - 25 Mbit/s
Uwaga: Średnia szybkość jest w szerokim zakresie zmienna i trudna do określenia		

Na podstawie analizy przedstawionych danych można zauważyć, że system HIPERACCESS musi funkcjonować tak, aby z perspektywy użytkownika był widziany jak system przewodowy. Użytkownik końcowy nie może być ograniczony faktem, że usługi są dostarczane poprzez kanał radiowy.

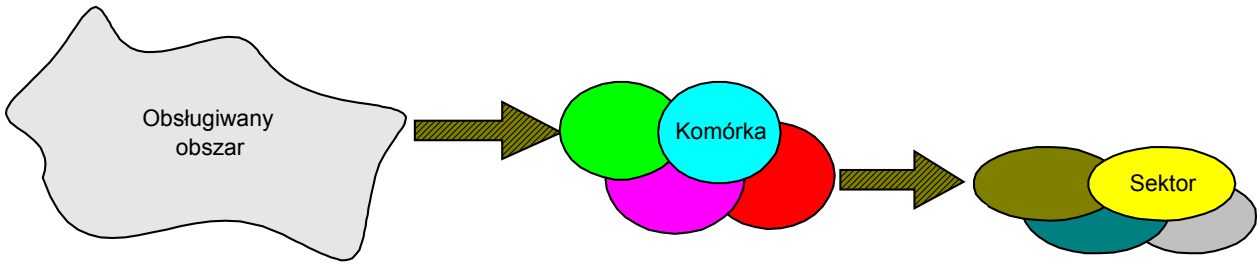
System HIPERACCESS oferuje transmisję danych o dużej szybkości (minimalna szybkość bitowa równa 25 Mbit/s.) zarówno "do" jak i "od" użytkownika z dynamicznym przydziałem pasma na żądanie. Przydzielane pasmo odpowiada szerokiemu zakresowi aplikacji w tym także usługom multimedialnym. W chwili obecnej na rynku istnieje wiele alternatywnych typów sieci spełniających przedstawione wymagania, zatem HIPERACCES będzie zmuszony konkurować z wieloma rozwiązaniami, a w tym:

- xDSL z wykorzystaniem instalacji miedzianej;
- Dystrybucyjne systemy mikrofalowe;
- TV kablowa;
- Modemy przewodowe;
- Systemy optyczne w budynkach i domowe (FTTB,FTTH).
- Instalacja elektryczna umożliwiająca realizację transmisji danych;

- Radiowa transmisja pakietowa;
- UMTS.
- Systemy satelitarne.

Jedną z wielu ważniejszych i konkurencyjnych zalet systemu HIPERACCESS w stosunku do alternatywnych rozwiązań jest jego krótki czas instalacji (deinstalacji). HIPERACCESS jest także dobrym technicznie i efektywnym ekonomicznie kandydatem uzupełniającym własności systemu UMTS. Uzupełnienie własności UMTS jest możliwe poprzez rozszerzenie obszaru pokrycia usługami (np. w miastach).

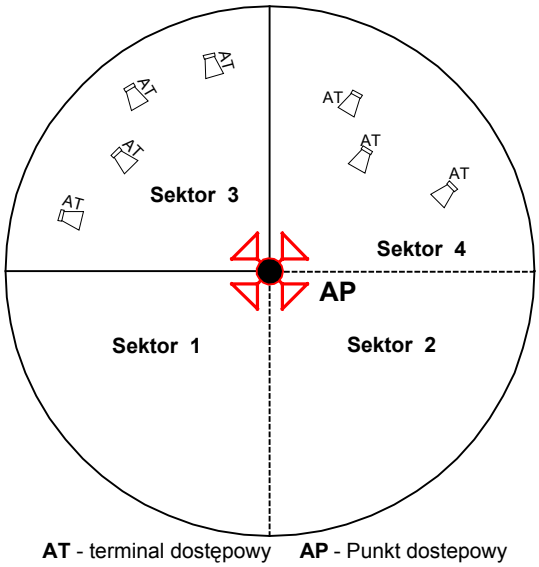
Typowa sieć HIPERACCESS składa się z kilku komórek, z których każda zapewnia pokrycie usługami części wyznaczonego rejonu. Hierarchia elementów organizacyjno - technicznych w obszarze obsługiwanym przez HIPERACCESS została przedstawiona na poniższym rysunku.



Rysunek 2.3.1. Hierarchia elementów organizacyjno - technicznych systemu HIPERACCESS

Przyjęta hierarchia elementów organizacyjno - technicznych w obszarze obsługi pozwala na rozwinięcie sieć HIPERACCESS w taki sposób, że może ona potencjalnie pokrywać rozległy obszar. Potwierdza to także fakt, że każda z komórek może funkcjonować w trybie "punkt - wiele punktów" (PMP), a urządzenia punktu dostępowego AP (często nazywane urządzeniami stacji bazowej - BS) umiejscawiane są w centralnym punkcie komórki.

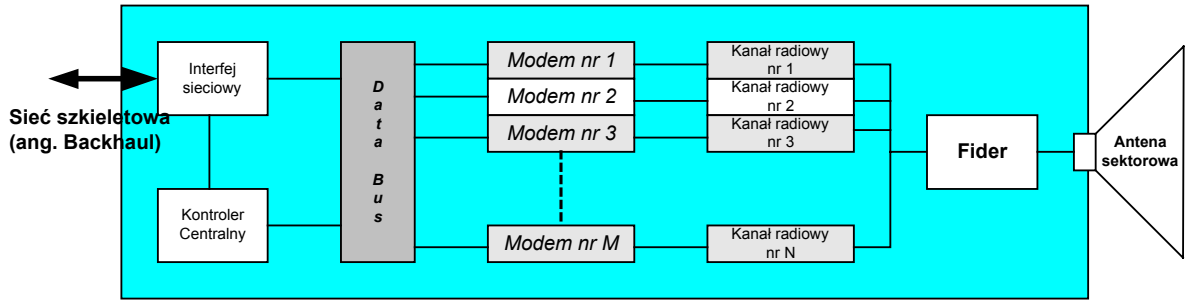
Punkt dostępowy AP może komunikować się z terminalami dostępowymi (AT) usytuowanymi we wnętrzu komórki. Zakłada się, że w ramach jej obszaru może funkcjonować do 256 urządzeń AT na sektor, przy wykorzystaniu do 254 częstotliwości nośnych. Konfigurację pojedynczej komórki z podziałem na 4 sektory przedstawiono na poniższym rysunku:



Rysunek 2.3.2. Przykład konfiguracji pojedynczej komórki z podziałem na 4 sektory obejmujące obszary po 90^0

Pojedyncza komórka jest podzielona na małą liczbę sektorów (np. 3 lub 4). Zastosowanie anten kierunkowych w AP zwiększa efektywność wykorzystania spektrum przez możliwość wielokrotnego zastosowania dostępnych kanałów radiowych (RF).

Schemat blokowy punktu dostępowego wykorzystywanego w systemie HIPERACCESS. przedstawiono na poniższym rysunku:

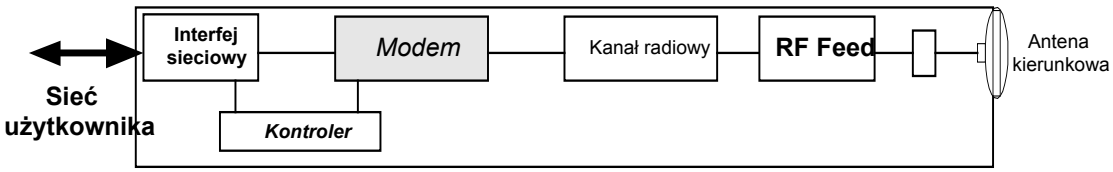


Rysunek 2.3.3. Schemat blokowy punktu dostępowego HIPERACCESS

Do podstawowych elementów składowych punktu dostępowego AP zalicza się antenę sektorową, modemy, kontroler centralny oraz interfejs do współpracy z siecią szkieletową.

AP zarządza typowo komunikacją w więcej niż jednym sektorze, zaś dla pokrycia obszaru każdego z nich jest wykorzystywana jedna lub więcej anten. Każde radiowe urządzenie nadawczo-odbiorcze komunikuje się z modemem zawierającym funkcje logiczne warstw PHY i DLC. Dane wysłane do albo odbierane od modemu są przenoszone poprzez magistralę danych. Sterownik centralny, komunikuje się i steruje modemy oraz bloki sprzęgające z siecią. Bloki te przenoszą dane z komórek do sieci szkieletowej.

Dla zachowania kompletności opisu podstawowych urządzeń występujących na najniższym poziomie systemy HIPERACCESS, przedstawiono przykładowy schemat blokowy terminala dostępowego AT występującego w systemie HIPERACCESS.



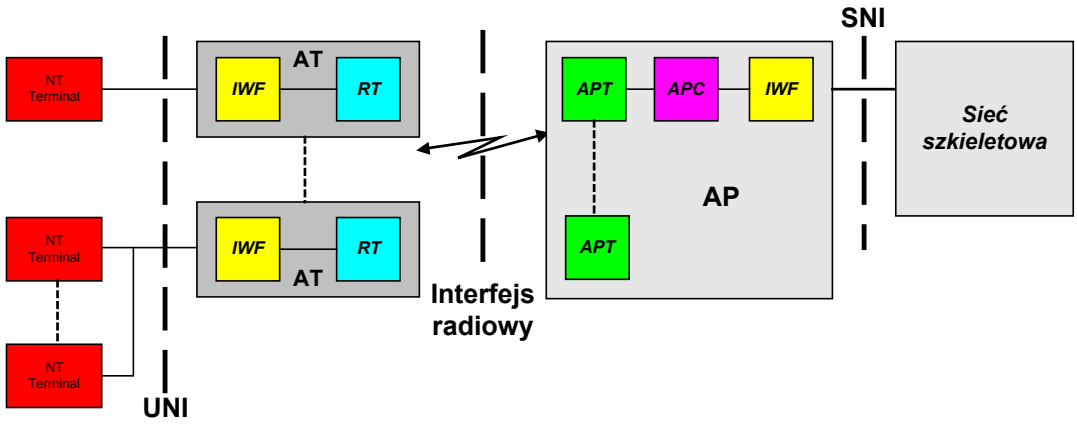
Rysunek 2.3.4. Schemat blokowy terminala dostępowego AT w systemie HIPERACCESS

Skład terminala AT jest zbliżony do składu przedstawionego przy opisie punktu dostępowego AP. Zmienione jest liczność elementów, ich funkcje oraz parametry techniczne. Np. w miejscu anteny sektorowej AP w AT występuje antena kierunkowa, a interfejs sieciowy nie jest odpowiedzialny za współpracę z siecią szkieletową, lecz z siecią użytkownika, która z technicznego punktu widzenia jest o wiele mniej skomplikowana.

Techniczne rozwiązania zastosowane w systemie HIPERACCESS umożliwiają współdzielenie kanałów RF pomiędzy wielu użytkowników (wewnątrz sektora). Podział łącza prowadzi do lepszej efektywności wykorzystania pasma i wzrostu pojemności systemu. Rozwiązane tego typu jest przeciwieństwem architektury typu "punkt - punkt", w której dzielenie łącza radiowego miedzy kilku abonentów sieci nie jest możliwe.

2.3.2 Aspekty sieciowe

Najistotniejsze bloki funkcjonalne oraz występujące w systemie HIPERACCESS interfejsy radiowe i przewodowe przedstawiono w formie graficznej na poniższym rysunku:



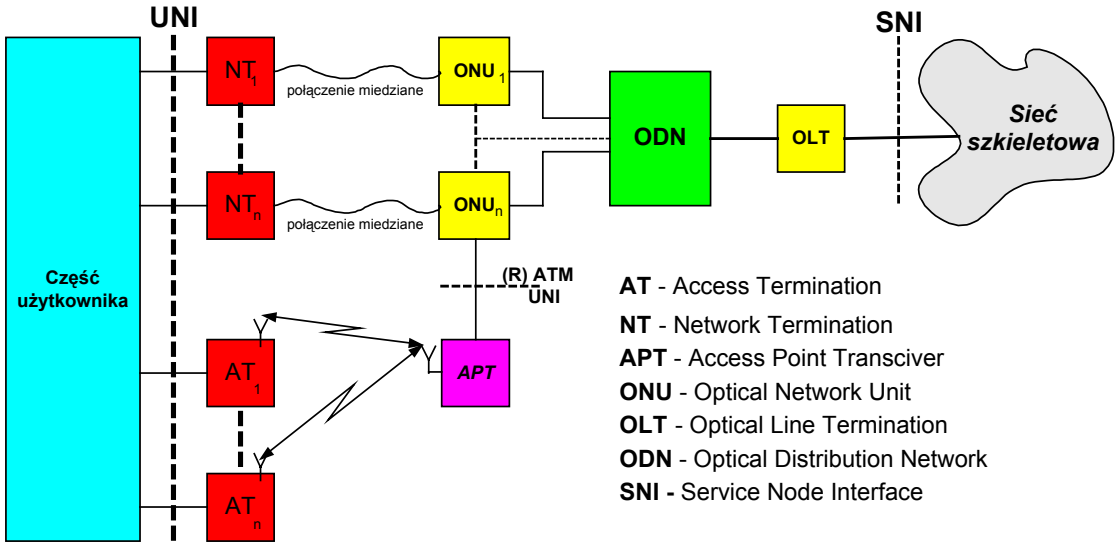
NT - Network Termination
AT - Access Termination
AP - Access Point
APT - Access Point Transciver
APC - Access Point TController
UNI - User Network Interface
SNI - Service Node Interface
IWF - Interworking Funktion
RT - Radio Termination

Rysunek 2.3.5. Podstawowa konfiguracja systemu HIPERACCESS

Głównymi elementami systemu są:

- Terminale dostępowe wraz ze stykiem UNI od strony terminali przewodowych oraz interfejsem radiowym od strony punktu dostępowego AP;
- Punkt dostępowy AP ze stykiem usługowym SNI od strony przewodowej sieci szkieletowej oraz interfejsem radiowym, przez który realizowana jest komunikacja AP z terminalem dostępowym.

Na kolejnym rysunku przedstawiono architekturę systemu HIPERACCESS połączonego z siecią szkieletową zrealizowaną w technice ATM przy wykorzystaniu połączeń światłowodowych.



Rysunek 2.3.6. Architektura systemu HIPERACCESS połączonego z siecią szkieletową typu ATM

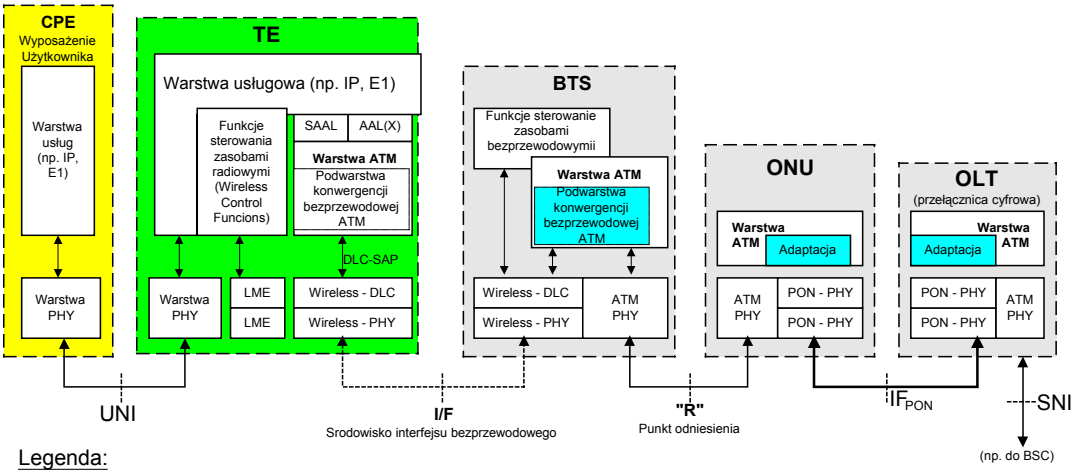
Na rysunku optyczne zakończenie łącza (OLT) łączy pasywną sieć optyczną PON przez interfejs SNI do węzłów usługi. Zakończenie OLT jest odpowiedzialne za zarządzanie wszystkimi specyficznymi aspektami PON związanymi z systemem transportowym ATM. ONU i OLT zapewniają przezroczysty transport usług ATM przez PON między interfejsami UNI i SNI.

W tabeli poniżej podano przykłady interfejsów do różnych typów sieci, z którymi system HIPERACCESS jest w stanie współpracować zarówno od strony styku UNI jak i od strony styku SNI. Od strony użytkownika na styku UNI (W.3) możliwa jest współpraca z całą gamą obecnie eksploatowanych technologii sieciowych poczynając od ISDN poprzez Ethernet, a na ATM kończąc. Od strony sieci szkieletowej na styku SNI (W.2) wymienione zostały znane styki umożliwiające podłączenie i współpracę z sieciami ISDN oraz ATM o przepływności 155 Mbit/s

Tabela 2.3.3: Rodzaje interfejsów dla dwóch różnych typów interfejsów sieci HIPERACCESS

UNI (W.3)	SNI (W.2)
Ethernet 10BaseT	VB5.1
ATMF25,6	VB5.2
E1 (fractional/not fractional)	V5.1
E1 ATM (G.804)	V5.2
ISDN BRA/PRA (I.430, I.431) POTS, ATMF 25M	155 ATM NNI/UNI

Opisana i przedstawiona w formie graficznej architektura sieci HIPERACCESS nie jest w stanie funkcjonować bez wykorzystania stosu protokołów zintegrowanego z optyczną siecią dostępową wykorzystującą technikę ATM. Stos ten zapewnia realizację pełnego zakresu usług FSAN - (ang. *Full Service Access Network*). Struktura OLT i funkcje są zdefiniowane w zaleceniu ITU - T serii G. 983.1 W sieci optycznej Optyczny Moduł Sieci (ONU) sprzęga zakończenie OLT przez interfejs IF_{PON} do styku UNI. Razem z OLT, ONU jest odpowiedzialny za przezroczysty transport usług ATM pomiędzy NNI i SNI.



Legenda:

CPE - wyposażenie użytkownika *(ang. Customer Premises Equipment)*
ONU - Optyczna jednostka sieciowa *(ang. Optical Network Unit)*
OTL - Optyczne zakończenie liniowe *(ang. Optical Line Terminator*
I/F_{PON} - Interfejs z pasywną siecią optyczną *(ang. I/F Pasive Optical Network)*
SNI - Interfejs zabezpieczeń sieciowych *(ang. Secure Network Interface)*
UNI - Interfejs użytkownika *(ang. User Network Interface)*
BTS - Stacja bazowa *(ang. Base Transceiver System)*
TE - Wyposażenie terminalu (*ang. Terminal Equipment)*
I/F - Interfejs
IP - Internet Protocol
E1 - ISDN strumień 2048 kbit/s

Rysunek 2.3.7.Stos protokołów systemu HIPERACCESS zintegrowanego z siecią dostępową

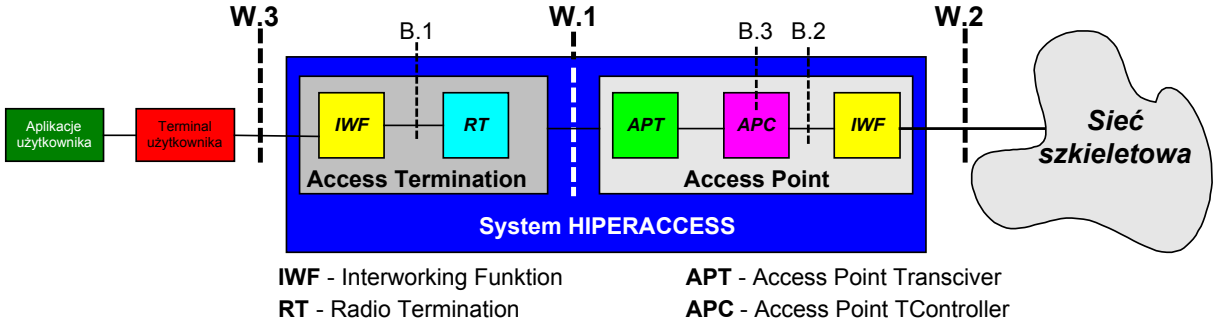
W zobrazowanej architekturze, protokoły transportowe ATM w interfejsie IF_{PON} są opisane jako składowe podwarstwy zależnej od medium fizycznego (PMD), podwarstwy zbieżności transmisji (TC) i warstwy ATM. Więcej szczegółów na ten temat można znaleźć np. w zaleceniu ITU - T serii I. 732.

2.3.3 Model odniesienia

W ramach techniczno - funkcjonalnej specyfikacji systemu HIPERACCESS wyróżnia się opisy:

- warstwy fizycznej - PHY;
- warstwy sterowania łączem danych - DLC;
- funkcji współpracy międzysieciowej zapewniające współpracę w punktach UNI i SNI;
- dwa typy funkcji współpracy międzysieciowej - IWF (ang. *InterWorking Functions*[6]) gdzie pierwszy typ IWF jest wymagany do tłumaczenia wewnętrznego interfejsu (B2) sieci HIPERACCESS na interfejs szczególnego rodzaju sieci szkieletowej takiej jak np. ATM. Inny typy IWF jest potrzebny do tłumaczenia wewnętrznego interfejsu (B1) sieci HIPERACCESS na zewnętrzny interfejs sprzętu terminala.

Wymienione rodzaje funkcji współpracy międzysieciowej zostały zilustrowane na poniższym rysunku, na którym przedstawiono model odniesienia systemu HIPERACCESS



Rys. 2.3.8. Model odniesienia systemu HIPERACCESS

Podobnie jak w przypadku ogólnego modelu systemu HIPERACCESS przedstawionego i omówionego wcześniej, w modelu obecnie prezentowanym wprowadzono i uszczegółowiono spis interfejsów występujących w systemie. Nazwy oraz podstawowe wymagania w stosunku do wspomnianych interfejsów przedstawiono w tabeli poniżej.

Tabela 2.3.4.: Wykaz i opis interfejsów występujących systemie HIPERACCESS

Styk	Opis	Wymagania
W1	Wewnętrzny interfejs bezprzewodowy	Będzie w pełni określony w standardach BRAN HIPERACCESS
W2	Zewnętrzny styk do sieci szkieletowej	Opracowany przez inne organizacje standaryzacyjne; wykaz interfejsów i współpracujących funkcji IWF został wyszczególniony w standardzie HIPERACCESS podwarstwy zbieżności
W3	Zewnętrzny interfejs do aplikacji/terminala użytkownika	Opracowany przez inne organizacje standaryzacyjne; wykaz interfejsów i współpracujących funkcji IWF został wyszczególniony w standardzie HIPERACCESS podwarstwy zbieżności
B1	Wewnętrzny usługowy interfejs zakończenia radiowego(AT)	Wyszczególniony tylko na poziomie logicznym, implementacja może ulegać zmianom.
B2	Wewnętrzny usługowy interfejs punktu dostępowego (AP)	Wyszczególniony tylko na poziomie logicznym, implementacja może ulegać zmianom.
B3	Interfejs - zewnętrzny element systemu zarządzania (EMS)	Stosowany jako znormalizowany dostępny protokół otwarty

[6] *IWFs są jednostkami logicznymi i nie posiadają szczególnej fizycznej lokacji w konfiguracji sieci HIPERACCESS*

2.3.4 Warstwa fizyczna PHY: modulacje i schematy kodowania

Rodzaj warstwy fizycznej PHY wstępnie jest zdefiniowany za pomocą łącznej kombinacji parametrów modulacji i kodowania. Architektura warstwy fizycznej jest określana głównie przez:

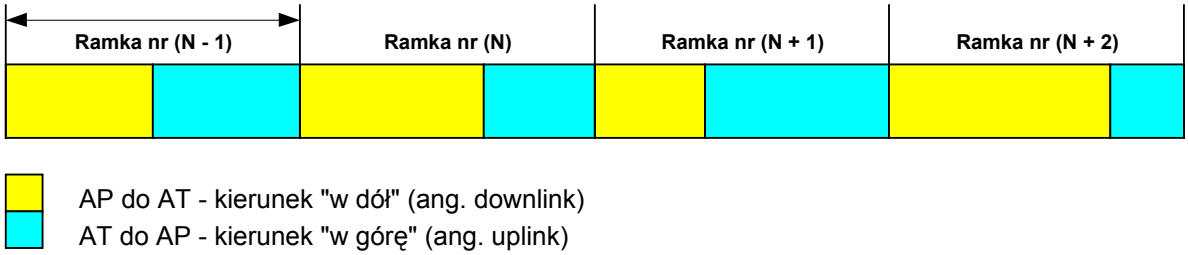
- Rodzaje transmisji - z pojedynczą falą nośną;
- Rodzaje wykorzystywanych schematów transmisji dupleksowych; FDD, H - FDD czy TDD;
- Rodzaj zastosowanego kodowania adaptacyjnego oraz rodzaj modulacji.

W systemie HIPERACCESS wykorzystywana jest modulacja **QAM**[7] z 2 ***M*** punktami konstelacji, gdzie ***M*** jest liczbą bitów transmitowanych w modulowanych symbolach. Dla łącza "w dół" jako obowiązująca wykorzystywana jest modulacja **QPSK** ($M = 2$) i **16QAM** ($M = 4$) natomiast jako opcjonalna przyjmowana jest modulacja **64QAM** ($M = 6$). Dla łącza "w górę" jako obowiązująca wykorzystywana jest modulacja **QPSK** natomiast modulacja **16QAM** występuje jako opcja.

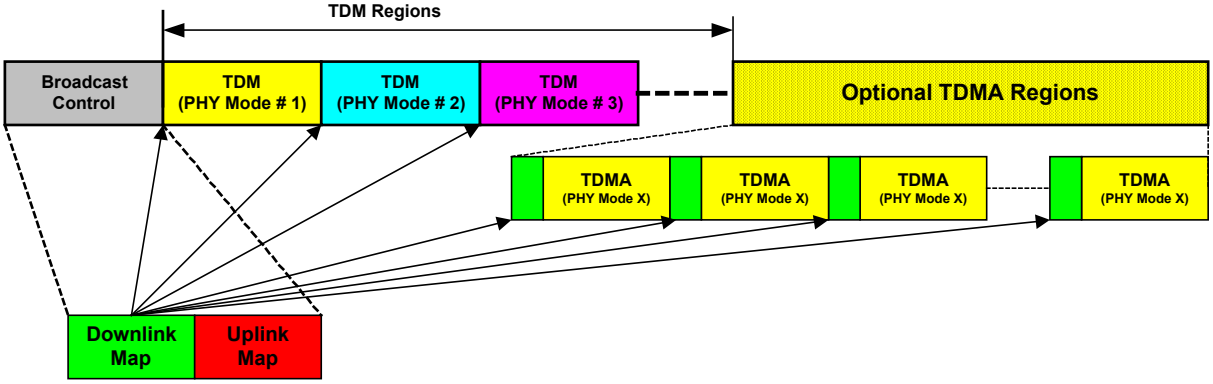
Schemat wyprzedzającej korekcji błędów (FEC) wykorzystuje kod Reed-Solomona z $t = 8$ i polem informacyjnym o długości 4 jednostek PDU skracany do wartości 3, 2 lub 1.

Kanał transmisji między AP i terminalami ATs jest dwukierunkowy, połączenie "w dół" (kierunek od AP do AT) DL i połączenie "w górę" (kierunek od AT do AP) UL.

Na poniższych rysunkach przedstawiono schemat ramki TDD w kierunku "w dół" oraz w kierunku "w górę" jak i podział ramki oraz multipleksacja w kierunku od AP do AT - DL.



Rysunek 2.3.9. Schemat ramki TDD w kierunku "w dół" oraz w kierunku "w górę"



Rysunek 2.3.10. Przykład sposobu podziału ramki i multipleksacji w kierunku od AP do AT

W systemie HIPERACCESS możliwe są do realizacji dwa typy trybów dupleksowych. Jeden z nich jest oparty na podziale w dziedzinie częstotliwości, a drugi na podziale w dziedzinie czasu. Dupleks z podziałem częstotliwości (FDD) dzieli będące w dyspozycji widmo w bloku połączenia "w górę" i bloku łącza "w dół". Kanał radiowy RF jest właściwie parą ścieżek - jednej z bloku połączenia "w górę" i jednej z blok łącza "w dół". Od momentu podziału na poszczególne bloki wszelkie połączenia są ustanawiane na rozłącznych i niezależnych kanałach radiowych. W HIPERACCESS przy wykorzystaniu systemu FDD zarówno kanały "w górę" jak i "w dół"

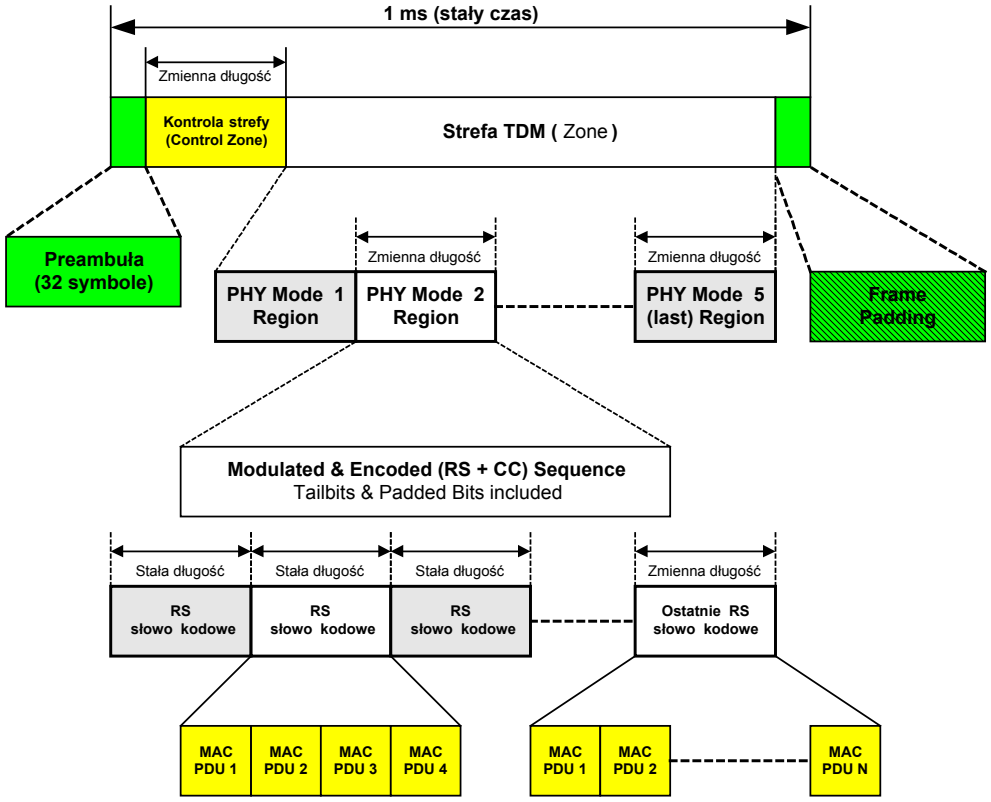
[7] *ang. Quadrature Amplitude Modulation*

zajmują pasmo 28 MHz. Wyposażenie terminala AT umożliwia także (jako opcja) realizację trybu pracy półdupleksowej w systemie FDD. Ten rodzaj pracy jest oznaczany jako H - FDD[8] (nadawanie i odbiór nie może występować równocześnie). W przeciwieństwie do FDD, drugi schemat transmisji dupleksowej dla połączenia "w dół" i "w górę" używa do komunikacji tego samego kanału RF z dupleksowym podziałem czasowy (TDD). Połączenie "w dół" i "w górę" są realizowane przez podział czasowym.

2.3.5 Technika multipleksacji

W systemie HIPERACCESS ten sam kanał RF jest wykorzystywany przez większą liczbę terminali AT. W takich sytuacjach punkt dostępowy AP musi wykorzystywać techniki sterowania dostępu do terminali AT. HIPERACCESS wykorzystuje technikę multipleksacji opartą na systemie TDMA (ang. *Time Division Multiple Access*).

Przykład odwzorowania jednostek PDU MAC do struktury PHY dla kierunku DL dla opcji zarówno "z" jak i "bez" TDMA został przedstawiony na poniższym rysunku.



Uwaga: N jest mniejsze lub równe 4

Rysunek 2.3.11.Transmisja PDUs MAC w łączu "w dół" dla opcji zarówno "z" jak i "bez" TDMA

Dane połączeń DL różnych ATs są multipleksowane w dziedzinie czasu (TDM). Ponieważ HIPERACCESS wykorzystuje tryby adaptacyjne w warstwie PHY, ramka składa się z kilku szczelin TDM. Każda szczelina TDM jest związana ze specyficznym rodzajem warstwy PHY. Tylko te terminale AT, które są zdolny odbierać (demodulować) przyporządkowany mu rodzaj PHY może znaleźć w zmultipleksowanej szczelinie TDM dane łącza DL. Aby uprościć proces demodulacji, szczeliny TDM są elastycznie umiejscawiane w porządku malejącym. Lokalizacja szczeliny TDM w ramce jest rozgłaszana w schemacie połączenia DL, na początku ramki.

[8] *Przy wykorzystaniu tego trybu pracy możliwa jest redukcja kosztów AT*

Harmonogram przesyłania danych dla transmisji "w górę" (UL) jest organizowany w sieci i rozgłaszany przez łącze "w dół" (DL). Łącze UL dla terminala AT zostanie zaplanowane przez AP po tym, jak AT zostanie zarejestrowany w systemie. Zaplanowane zdarzenia będą bazować na koordynacji czasowej definiowanej wtedy, gdy AT rozpoczyna i kończy transmisję.

AT może nadawać w sposób niezapowiedziany tylko w dwóch następujących przypadkach:

- W celu zarejestrowania się;
- W odpowiedzi na zapytania w trybie do wszystkich z grupy i rozgłoszeniowym.

Do zasadniczych własności DLC[9]. W systemie HIPERACCESS zalicza się:

- Efektywne wykorzystywanie pasma;
- Wysoki zysk multiipleksacji;
- Obsługiwanie QoS.

Zwielokrotnianie oznacza, że *m* użytkowników może współdzielić *n* kanałów radiowych (gdzie *m* jest większe niż *n*). Zastosowanie tego typu rozwiązania wymaga użycia rozproszonego inteligentnego sterowania, które pozwala na realizacje wiele różnorodnych działań i realizacji funkcji obsługowych (zarządzających). Warstwa DLC jest zorientowana połączeniowo, (co oznacza, że PDUs MAC są odbierane w takim porządku, w jakim zostały nadane i że połączenie jest zestawiane przed wysłaniem jednostek PDU MAC), co gwarantuje utrzymanie wymaganych parametrów QoS. Połączenia są zestawiane z wykorzystaniem kanału radiowego poprzez zainicjowanie terminala AT. Nowe połączenia mogą być zestawiane wtedy, kiedy wymagana jest realizacja nowej usługi.

2.3.6 Podsumowanie

Przedstawione zasadnicze elementy związane z funkcjonowaniem systemu HIPERACCESS oraz własności tego systemu wskazują, że w najbliższym czasie może on odegrać znaczącą rolę w zapewnianiu usług zwłaszcza dla indywidualnych użytkowników domowych, właścicieli prowadzących małej i średniej wielkości przedsięwzięcia gospodarcze oraz w tych typach infrastruktur sieci mobilnych, które wymagają realizacji usług telekomunikacyjnych związanych ze spędzeniem wolnego czasu, rekreacją czy rozrywką.

HIPERACCESS w opisanym kształcie będzie ulegał pewnym modyfikacjom. Głównie przejawiać się będzie to w rozszerzeniu współpracy z siecią UMTS z jednej strony (interfejs SNI) a od strony wyposażenia abonenta (interfejs UNI) z poszerzeniem liczby interfejsów umożliwiających współpracę z liczną grupą sieci o dużych przepływnościach.

[9] *Zobacz ETSI: TS 101 999, TS 102 000*

2.4 Bezprzewodowy system dostępowy ATM - WACS

Prace nad nowymi technologiami sieci WLAN zmierzają w dwóch kierunkach:

- opartym na rozwiązaniach sieci dopuszczających transmisję ramek o zróżnicowanych długościach;
- związanym ze specyfikacją rozwiązań sieciowych wykorzystujących jako podstawową jednostkę danych przesyłanych między użytkownikami komórkę ATM

Jednym z bardzo istotnych typów sieci współpracujących z trzema różnymi aplikacjami sieci HIPERLAN opracowanych w ramach projektu BRAN (ang. *Broadband Radio Access Networks*) jest sieć oparta na technice ATM. W ramach rozwiązywania problemów kompatybilnego współdziałania sieci HIPERLAN z sieciami ATM opracowano specyfikację dla bezprzewodowego systemu dostępowego ATM (WACS - *ang. Wireless ATM Access Systems*)[10]. Sieć tego typu jest nazywana także systemem dostępowym ATM. Specyfikacja jest uzgodnieniem pomiędzy takimi organizacjami jak ETSI i ATM Forum, w której ETSI dokonał opracowania odpowiedniej warstwy fizycznej oraz warstwy łącza danych, natomiast warstwy wyższe zostały przyjęte jako opracowania ATM Forum. Zadaniem tak skonstruowanego systemu jest zapewnienie lokalnego i zdalnego[11] bezprzewodowego dostępu do sieci ATM w ramach, którego możliwa jest realizacja następujących usług:

- Zestawianie połączeń zgodnych ze specyfikacją sygnalizacji ATM w tym wspomaganie zarządzania ruchem i zapewnianiem odpowiednich parametrów jakościowych;
- Obsługa połączeń wychodzących i przychodzących;
- Monitorowanie stanu łączy radiowych i wskazywanie zmian w środowisku radiowym oraz dynamiczną alokację zasobów łącza radiowego odpowiednio do warunków wynegocjowanego kontraktu ruchowego;
- Wspomaganie ochrony źródła zasilania stacji mobilnej (np. tryb uśpienia);
- Szyfrowanie danych przenoszonych w łączu radiowym.

2.4.1 Model odniesienia

Dla bezprzewodowego systemu dostępowego ATM (WACS) zdefiniowano dwa rodzaje modeli odniesienia, które nazwano:

- Model ze sterowaniem rozproszonym (*ang. Distributed Control Model*);
- Model ze sterowaniem skupionym (jednorodnym) (*ang. Unified Control Model)*.

Opracowane modele tworzą odpowiednio połączone elementy funkcjonalne rozdzielone wyróżnionymi punktami nazywanymi punktami odniesienia. W realizacjach fizycznych punkty odniesienia mogą stanowić odpowiednie interfejsy.

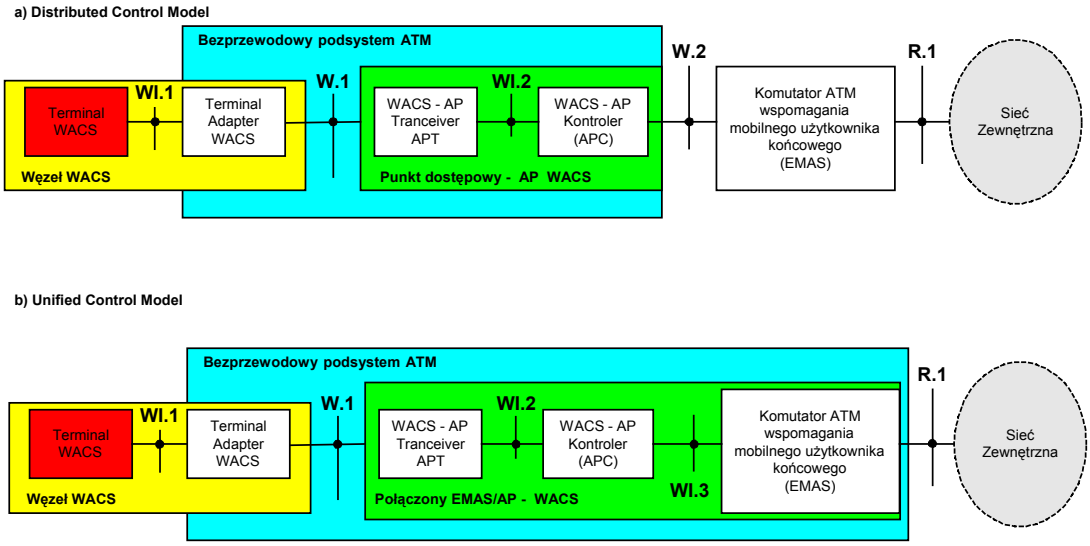
Do elementów funkcjonalnych modeli odniesienia należą:

- Węzeł (stacja) WACS, w składzie, której wyróżniono terminal oraz adapter WACS;
- Punkt dostępowy WACS, w którym po dekompozycji wyróżnia się sterownik punktu dostępowego oraz jeden lub kilka nadawczo/odbiorczych punktów sterowanych przez sterownik punktu dostępowego - APC;
- Funkcje komutatora ATM wspomagające końcowego użytkownika mobilnego.

[10] *WACS nazywany jest także jako podsystem dostępowy ATM.*

[11] *Dostęp lokalny w znaczeniu telekomunikacyjnym oznacza krótki zasięg (mniej niż 100 m) bezprzewodowego dostępu do innych możliwych sieci przewodowych, natomiast zdalny dostęp oznacza długi zasięg (do 10 km).*

Wymienione elementy funkcjonalne zostały przedstawione na rysunku 2.4.1 a i b. Jak można zauważyć model zunifikowany (jednorodny) jest uproszczeniem modelu rozdzielonego. W obu modelach określono jednakowy typ interfejsu radiowego. Różnica między modelami przejawia się w połączeniu funkcji interfejsów W.2 i wewnętrznego interfejsu WI.3



Rys. 2.4.1. Dwa typy modeli odniesienia bezprzewodowego dostępu dla systemów ATM

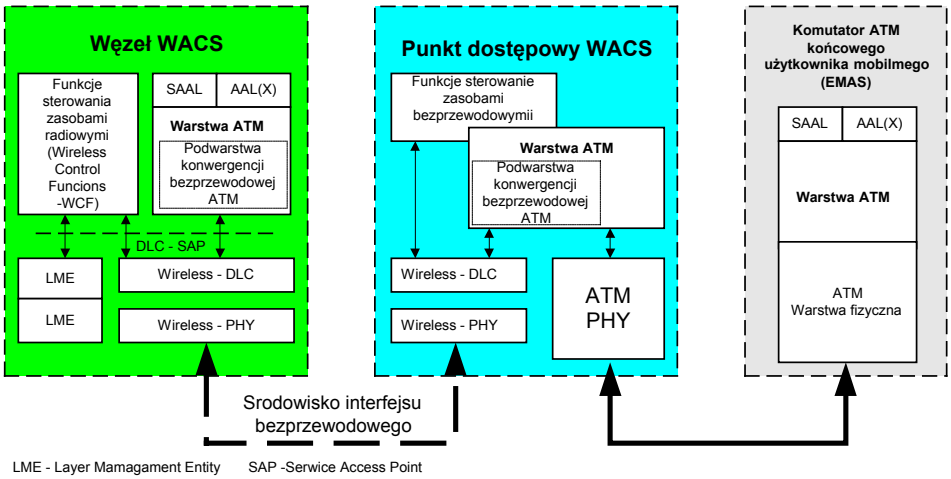
W modelu pierwszym (rozdzielonym) umiejscowione są mechanizmy i funkcje zapewniające przekazywanie wędrujących stacji mobilnych pomiędzy punktami dostępowymi sieci. Przedstawione modele nie muszą koniecznie posiadać fizycznych implementacji w każdym z trzech typów aplikacji sieci HIPERLAN. I tak np., przedstawiony na rysunku 2.4.1 a) węzeł WACS stanowi jedną całość, w którym interfejs WI.1 jest interfejsem wewnętrznym tego węzła. W rzeczywistych aplikacjach HIPERACCESS terminal adapter może być umieszczany zarówno w terminalu użytkownika jak i w sieci.

Tabela 2.8. Punkty odniesienia. Wykaz z opisem

Lp.	Punkt odniesienia	Opis
1.	**W.1**	Interfejs radiowy, który zawiera: • Protokoły warstwy DLC zapewniające przezroczysty transport ruchu ATM w płaszczyznach U, C, M na takim poziomie jak umożliwiają to funkcje wspomagające mobilność i bezpieczeństwo w tym szyfrowanie informacji; • Protokół UNI - z rozszerzeniem uwzględniającym mobilność zgodną z implementacjami ATMF oraz jako opcja rozszerzenie o ILMI
2.	**W.2**	Interfejs pomiędzy punktem dostępowym WACS AP i EMAS wraz z jego funkcjami zarządzania i sterowania, który zawiera protokół sterowania punktem dostępowym WACS. Protokół ten. przenosi interakcje pomiędzy WACS AP i EMAS dla ustanawianych i zwalnianych połączeń, dla połączeń przenoszonych pomiędzy poszczególnymi AP sieci. Specyfikacja protokołu zależy od sposobu rozdzielenia funkcji miedzy AP i EMAS
3.	**R.1**	Interfejs standardowy pomiędzy EMAS i siecią zewnętrzną zapewniający rozszerzenie o funkcje mobilności, np. (M-) UNI lub (M-) NNI.
4.	WI.1	Wewnętrzny interfejs węzła WACS - nie jest przedmiotem zaleceń.
5.	WI.2	Wewnętrzny interfejs punktu dostępowego WACS - nie jest przedmiotem zaleceń.
6.	WI.3	Wewnętrzny interfejs połączonych elementów EMAS/AP - nie jest przedmiotem zaleceń.

2.4.2 Warstwowy model protokołów bezprzewodowej sieci ATM

W celu realizacji funkcji przedstawionych w rozdzielonym modelu sterowania (rys. 2.4.1 a) został opracowany stos różnorodnych protokołów. Protokoły te zostały odpowiednio uszeregowane i przedstawione w postaci modelu warstwowego na rysunku 2.4.2.



Rys. 2.4.2. Architektura warstwowa protokołów bezprzewodowego systemu ATM

W architekturze protokołów bezprzewodowego systemu ATM przedstawionej na rysunku występują trzy elementy funkcjonalne tj. węzeł WACS, punkt dostępowy WACS oraz komutator ATM. We wszystkich elementach funkcjonalnych umiejscowiono protokoły służące do transportu danych użytkownika oraz protokoły związane z sygnalizacją oraz zarządzaniem zapewniające współpracę z siecią ATM przy wykorzystaniu środowiska zarówno bezprzewodowego jak i przewodowego.

W zależności od funkcji elementu w systemie posiada on zróżnicowaną warstwową architekturę protokołów. Węzeł WACS komunikujący się z komutatorem ATM poprzez punkt dostępowy WACS wykorzystuje protokoły:

- warstwy fizycznej umożliwiające komunikację z wykorzystaniem wolnej przestrzeni;
- warstwy łącza danych do współpracy z medium bezprzewodowym;
- warstwy ATM umożliwiające dostęp do zasobów sieci ATM;
- kilku klas warstw adaptacyjnych ATM tj. SAAL służąca do obsługi podsystemu sygnalizacji ATM oraz AAL X gdzie X przyjmuje wartości od 1 do 5 w zależności od obsługiwanej klasy ruchu ATM np. DBR, SBR, ABR itp.;
- jednostek zarządzania warstwą (LME) na poziomie warstwy fizycznej i łącza danych oraz stosu protokołów związanych ze sterowaniem mobilnością (WCF)

Punkt dostępowy WACS w odróżnieniu do węzła WACS nie posiada protokołów wchodzących w skład LME oraz warstwy adaptacyjnej ATM, ale posiada dodatkowo protokoły warstwy fizycznej ATM. Ostatni z wymienianych elementów systemu tzn. komutator ATM posiada stos protokołów ATM poczynając od warstwy fizycznej a na kilku klasach warstw adaptacyjnych ATM kończąc. Ich uproszczona specyfikacja obejmuje przedstawione poniżej składniki.

2.4.3 Zarządzanie mocą

Stosowane są dwa tryby zmierzające do efektywnego wykorzystania dysponowanej mocy:

- tryb nazywany jako *"p-saver"* - porządkujący i optymalizujący czas niezbędny do odbioru danych;
- tryb nazywany jako *"p-supporter"* - porządkujący interwały czasowe i optymalizujący czas niezbędny do przekazania (transferu) danych.

2.4.4 Bezpieczeństwo

W HIPERLAN zakłada się szyfrowanie/ deszyfrowanie danych i do tego celu przewidziany jest pojedynczy algorytm, który wymaga identycznego klucza i wektora inicjującego zarówno proces szyfrowania jak i deszyfrowania. Nie określono szczegółowych metod kryptograficznych, ale zdefiniowano metody informowania odbiornika, którego klucza kryptograficznego użyto by zaszyfrować dany pakiet. Określono także zasady przechowywania niewielkiego zasobu kluczy w węźle. Strategia dystrybucji kluczy znajduje się poza zasięgiem standardu.

3 Standard IEEE 802.11

Standard IEEE 802.11 jest promowany przez komitet standardów sieci lokalnych i metropolitalnych (LMSC - ang. *Local and Metropolitan Area Networks Standards Committee*) IEEE Computer Society. Zanim standard został zatwierdzony w czerwcu 1997 r. poprzedziło go sześć wersji roboczych. W ostatecznym kształcie standard został uznany także jako zarówno standard IEEE jak i ISO/IEC oraz pozwala dużej liczbie producentów i sprzedawców rozwinąć szeroką gamę urządzeń dla powszechnie dostępnego pasma 2,4 GHz ISM (ang. *Industrial, Scientific, and Medical*).

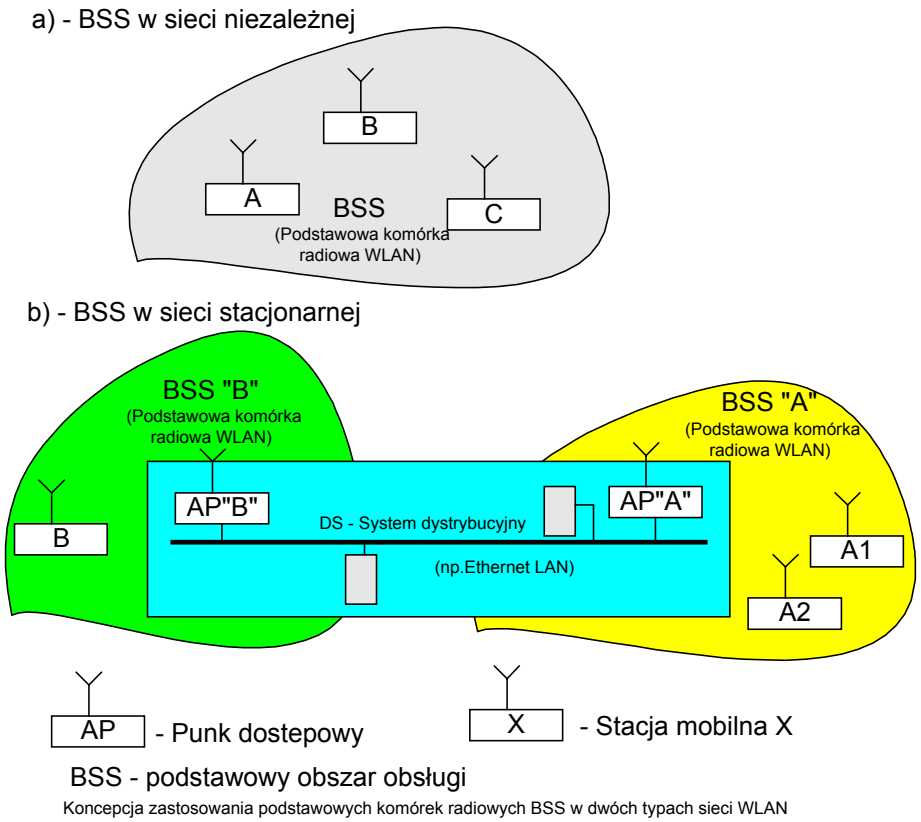
Standard IEEE 802.11 określa zasady bezprzewodowej pracy urządzeń stałych, przenośnych i węzłów ruchomych w geograficznie ograniczonym obszarze. W szczególności definiuje interfejs pomiędzy bezprzewodowym klientem a punktem dostępu (AP) jak również interfejs pomiędzy bezprzewodowymi klientami. Podobnie jak w innych standardach IEEE 802.x jak np. 802.3, standard 802.11 definiuje warstwę fizyczną (PHY) oraz sterowania dostępem do medium (MAC). Warstwa MAC w 802.11 spełnia funkcje, które zazwyczaj są skojarzone z wyższymi warstwami protokołu (np. fragmentacja, poprawianie błędów, zarządzanie mobilnością czy oszczędzanie energii. Te dodatkowe funkcje pozwalają warstwie MAC standardu 802.11. ukrywać unikalne cechy warstwy fizycznej przed wyższymi warstwami.

W literaturze związanej z sieciami WLAN spotyka się odwołania do następujących dokumentów: IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11h. Obecnie jako standardy zostały przyjęte następujące dokumenty IEEE: IEEE 802.11. jako dokument główny, oraz jako załączniki do wspomnianego dokumentu IEEE 802.11a oraz IEEE 802.11b. Pozostałe dokumenty jak np. IEEE 802.11g. został przedstawiony jako wersja robocza w październiku 2002 r. a IEEE 802.11h. znajduje się w fazie standaryzacji.

Wymienione dokumenty dotyczą różnych odmian WLAN. Na przykład IEEE 802.11b, dotyczy sieci o przepływności 11 Mbit/s w której zaleca się wykorzystywanie wielofazowego ciągu rozpraszającego. Z kolei IEEE 802.11a. przedstawia działanie systemu o przepływności do 54 Mbit/s w paśmie 5 GHz oraz zakłada stosowanie bardzo efektywnej modulacji wielotonowej OFDM (ang. *Ortogonal Frequency Division Multiplexing*). Jak wspomniano IEEE 802.11g. został przedstawiony jako wersja robocza w październiku 2002 r. a dotyczy opisu działania systemu analogicznego jak opisano w IEEE 802.11a., lecz funkcjonującego w paśmie 2,4 GHz. Jest on kompatybilny ze standardem IEEE 802.11a. Jeżeli chodzi o dokument IEEE 802.11h. znajdujący się w fazie standaryzacji zakłada dynamiczny wybór kanału i sterowanie mocą urządzeń działających w paśmie 5 GHz.

3.1 Architektura sieci i model odniesienia (IEEE 802.11)

W standardzie bezprzewodowej sieci LAN IEEE 802.11 podstawową jednostką organizacyjną jest BSS (ang. *Basic Service Set*). BSS stanowi rodzaj komórki radiowej WLAN, w skład której wchodzą dwie lub więcej stacji (nazywanych także węzłami mobilnymi). Na rysunku 3.1 zilustrowano koncepcję BSS, które należą do bezprzewodowej sieci niezależnej (nazywanej także tymczasową lub *ad hoc*) oraz bezprzewodowej sieci z infrastruktura (nazywana także siecią stałą).



Rys. 3.1. Architektura bezprzewodowej sieci LAN IEEE 802.11

Każda BSS posiada identyfikator nazywany BSSID który odpowiada adresowi MAC bezprzewodowej karty będącej częścią sieci. Obszar, w którym może być realizowana łączność bezprzewodowa przez składowe BSS nazywany jest podstawowym obszarem pokrycia BSA (ang. *Basic Service Area*). Niezależna sieć zawierająca tylko jedną BSS jest oznaczana jako IBSS (ang. *Independent BSS*), natomiast system DS łączący dwie lub więcej BSS w jedną całość (najczęściej poprzez siec szkieletową) tym samym udostępnia zasoby sieci stałej. WLAN zawierający zbiór BSS i DS jest nazywany jako rozszerzona komórka ESS (ang. *Extended Service Set*). Zatem dane BSS i ESS także posiadają unikalny identyfikator nazwany ESSID. Zdefiniowanie wspólnego ESSID pozwala stacjom przemieszczać się z jednej BSS do innej.

3.2 Podstawowy model odniesienia

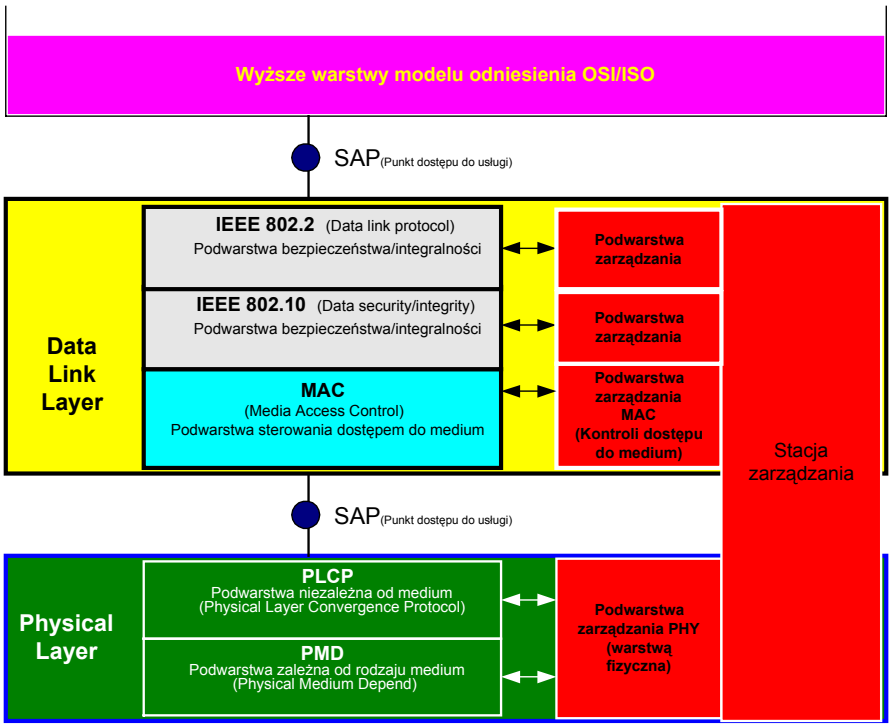
Na rysunku 3.2 przedstawiono podstawowy model odniesienia IEEE 802.11. Na wspomnianym rysunku warstwa fizyczna została podzielona na dwie podwarstwy. Podwarstwa zależna od medium (PMD) współpracuje z charakterystycznymi dla bezprzewodowej sieci mediami tj. DSSS, FHSS lub DIFIR i określa metody nadawania i odbioru danych (np. modulacja, kodowanie). Druga z podwarstw warstwy fizycznej tj. niezależna od medium PLCP określa metodę odwzorowania jednostki danych protokołu podwarstwy MAC (MPDUs) w format pakietu dogodny dla podwarstwy PMD. Na poziomie warstwy łącza danych wyróżniono podwarstwę sterowania dostępem do medium MAC, która to podwarstwa określa podstawowy mechanizm dostępu (bazujący na protokole CSMA/CA, który jest zaadaptowaną do warunków środowiska radiowego wersją CSMA/CD) do medium dla wielu stacji. Podwarstwa ta może także dokonywać fragmentacji i szyfrowania pakietów danych.

Zarządzanie warstwą fizyczną koncentruje się głównie na adaptowaniu zmiennego stanu łącza i obsługiwaniu bazy informacyjnej (MIB). Podwarstwa zarządzania MAC zajmuje się synchronizacją zarządzaniem mocą, łączeniem/rozłączaniem. Ostatecznie stacja pracy zarządzania określa w jaki sposób warstwa fizyczna (PHY) i podwarstwy MAC współpracują z innymi warstwami.

3.2.1 Warstwa fizyczna

Specyfikacja warstwy fizycznej dopuszcza trzy opcje transmisji, które umożliwiają bezprzewodowym sieciom LAN 80.11 rozwijać się w różnych obszarach poczynając od pojedynczego pokoju a na całych campusach kończąc. Do tych opcji należą:

- fale radiowe z rozpraszaniem widma metodą kluczowania bezpośredniego - DSSS (ang. *Direct Sequence Spread Spectrum*);
- fale radiowe z rozpraszaniem widma metodą przeskoków częstotliwości - FHSS (ang. *Frequency Hopping Spread Spectrum*);
- fale optyczne z zakresu podczerwieni DFIR (ang. *Diffuse Infrared*).



Rys. 3.2 Model odniesienia IEEE 802.11 dla WLANs

W celu poprawnej pracy WLAN 802.11 poszczególne urządzenia powinny wykorzystywać w pracy tą samą warstwę PHY (np. WLAN z FHSS powinien współpracować z innym WLAN też z FHSS a nie z WLAN DSSS). Kiedy PHY operuje na DFIR dwie opcje radiowe (DSSS FHSS) operują w paśmie ISM 2,4 GHz. Operowanie w tym paśmie nie wymaga od użytkownika posiadania specjalnej licencji. Specyfikacja 802.11 DSSS obligatoryjnie przeznaczona jest do realizacji przepływności 1 i 2 Mbit/s. Dla specyfikacji FHSS i DFIR obligatoryjną przepływnością 1 Mbit/s natomiast przepływność 2 Mbit/s jest opcją.

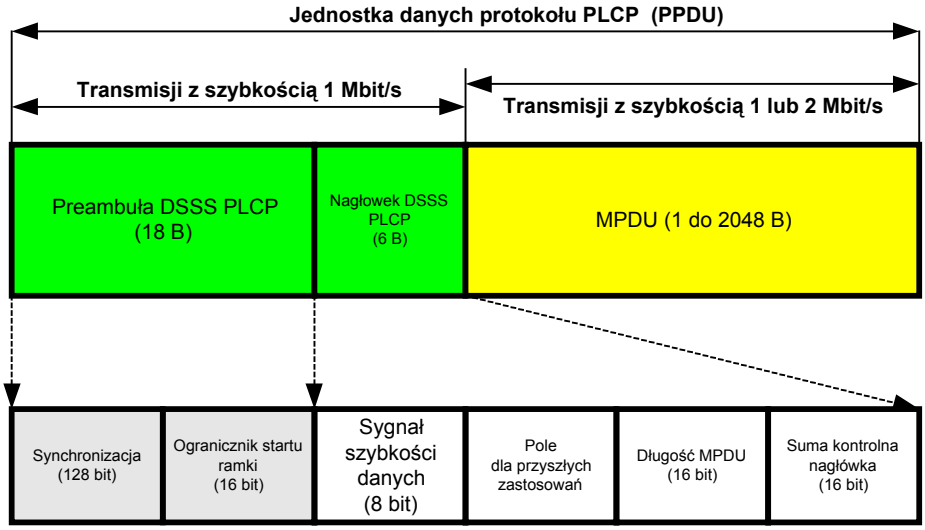
3.2.2 Format pakietów

Informacje użytkownika są dzielone na pakiety danych z preambułą PLCP i nagłówkiem PLCP dołączanym na początku pakietu. W tym miejscu należy zaznaczyć, że w standardzie 802.11 w miejsce pakietów danych preferuje się nazwę ramki (ang. *frames*).

Po odebraniu węzeł synchronizuje według preambuły PLCP otrzymując długość pakietu danych przepływność (np. 1 lub 2 Mbit/s) oraz inne informacje zawarte w nagłówku PLCP. Należy zaznaczyć, że preambuła i nagłówek PLCP są transmitowane z szybkością 1Mbit/s. To pozwala WLAN 802.11 o niższej szybkości współpracować z WLAN 802.11 o wysokiej szybkości.

Format pakietu dla DSSS 802.11 został przedstawiony na rys. 3.3. Nazwy poszczególnych pól nagłówka PLCP wyjaśniają ich przeznaczenie. Pozwalają one węzłowi odbiorczemu wykryć sygnały autokorelacji pseudokodu i zapisywać czas przybycia pakietu, a bity synchronizacyjne

umożliwiają wybór odpowiedniej anteny, (jeżeli wybór istnieje). Pole sygnału wskazuje czy MPDU była modulowana przy pomocy DBPSK (1 Mbit/s) czy DQPSK (2 Mbit/s). Może zostać także użyty do oznaczenia wyższych przepływności, które mogą pojawić się w przyszłości. Ogranicznik startu ramki wskazuje początek pakietu danych. Pole długości pakietu określa długość MPDU, podczas gdy pole sumy kontrolnej zabezpiecza trzy pola nagłówka PLCP.



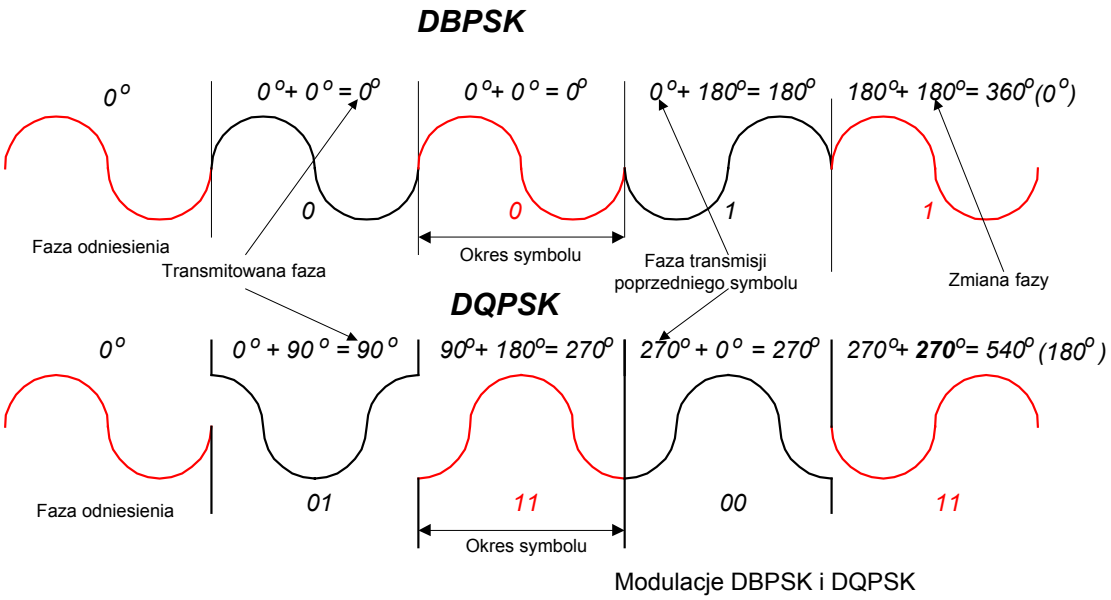
Rys. 3.3. Format pakietu DS SS PLCP

Przy przepływności 1 Mbit/s stosowana jest modulacja DBPSK (ang. *Differential Binary Phase Shift Keying*) gdzie każdy bit danych jest odwzorowywany w jedną z dwóch faz. Przy przepływności 2 Mbit/s wykorzystuje się modulację DQPSK (ang. *Differential Quadrature Phase Shift Keying)*. W tym przypadku dwa bity danych są odwzorowywane za pomocą czterech faz kodu rozpraszającego. W tabeli przedstawiono definicje faz dla wymienionych rodzajów modulacji.

Tabela 3.2. Definicje fazy dla DBPSK i DQPSK

Modulacja	Dane	Zmiana fazy
DBPSK	0 1	0^0 180^0
DQPSK	00 01* 11 10*	0^0 90^0 180^0 270^0
)* - najstarszy bit jest transmitowany jako pierwszy		

W DBPSK, informacja jest kodowana w oparciu o różnice faz sąsiednich symboli danych. Innymi słowy transmitowana faza (Φ_n) symbolu jest funkcją poprzedniej fazy (Φ_{n-1}) i zmiany fazy ($\Delta\Phi_n$) w wyniku: ($\Phi_n = \Delta\Phi_n + \Phi_{n-1}$). Uzyskuje się różne fazy w minimalnym czasie. uzyskują minimalne czasy. Schemat funkcjonowania modulacji DBPSK i DQPSK zilustrowano na rys. 3.4.

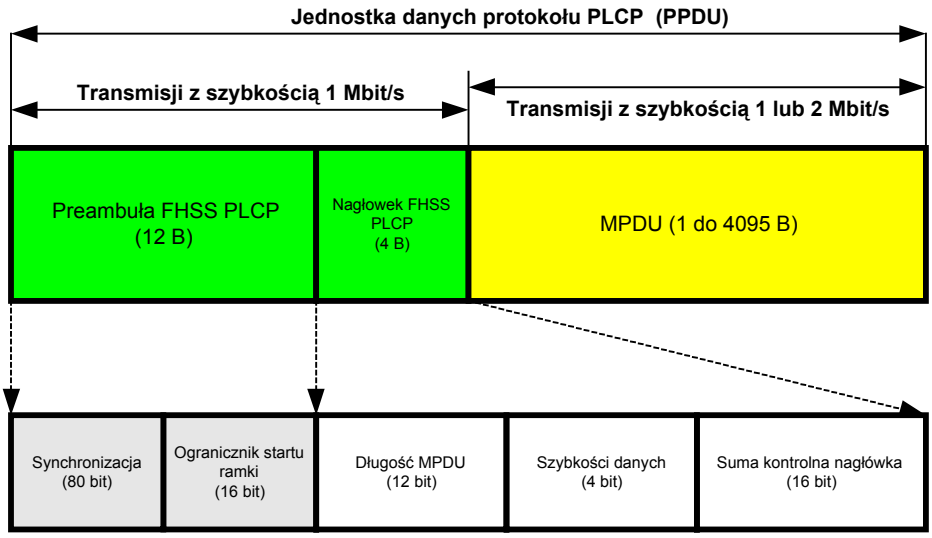


Rys. 3.4. Schemat funkcjonowania modulacji DBPSK i DQPSK

Specyfikacja DSSS 802.11 wymaga, aby były zaimplementowane obie szybkości transmisji. Odbierany sygnał wejściowy został określony na poziomie - 80 [dBm] dla pakietowej stopy błędów - PER (ang. *packet error rate*) 8 x 10^{-2}. PER jest definiowane jako prawdopodobieństwo nie zdekodowania wszystkich bitów w poprawnym pakiecie danych. Jego wartość zależny od wielkości bitowej stopy błędów (BER) oraz długości pakietu. Wykorzystywany kod Barker'a wykazuje dobre własności autokorelacji - jest relatywnie krótki co pozwala na szybką synchronizację.

3.2.2.1 *Warstwa fizyczna FHSS*

Format pakietu warstwy fizycznej z FHSS przedstawia poniższy rysunek.



Rys. 3.5. Format pakietu warstwy fizycznej z FHSS

Dokonując porównania formatu pakietów PLCP DSSS i FHSS można zauważyć, że w stosunku do PLCP DSSS, w pakiecie FHSS PLCP występuje mniejsze pole synchronizacji (80 w stosunku do 128 bit przy DSSS PLCP) oraz mniejszy jest o 2 bajty nagłówek PLCP FHSS. Można także zauważyć, że maksymalna długość pola MPDU DSSS jest mniejsza w porównaniu do odpowiedniej MPDU FHSS.

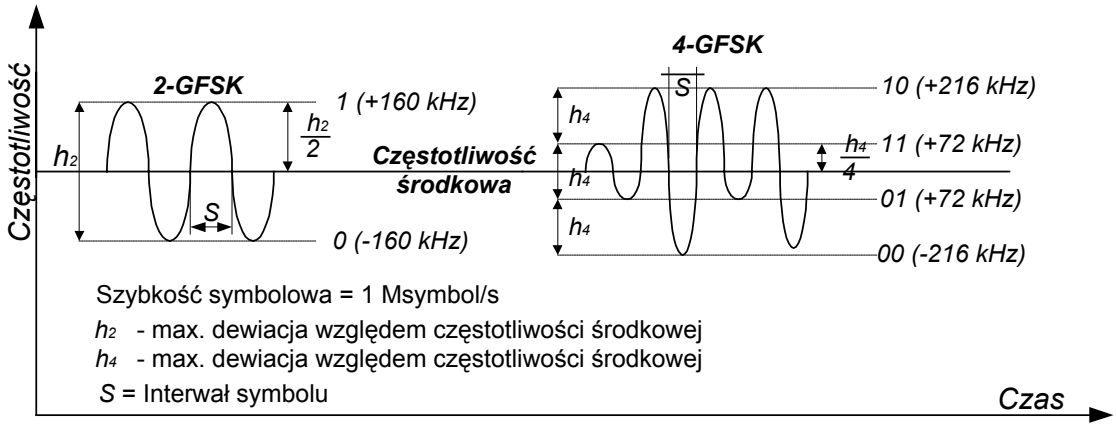
Przy przepływności 1 Mbit/s zastosowano modulację 2-GFSK (ang. *2-level Gaussian Frequency Shift Keying*), w której każdy bit danych jest odwzorowywany na jedną z dwóch częstotliwości. Przy przepływności 2 Mbit/s, która jest opcjonalna, wykorzystuje się modulację 4-GFSK. W tym przypadku dwa bity danych są odwzorowywane z wykorzystaniem jednej z czterech częstotliwości. Odfiltrowane dane są następnie modulowane z wykorzystaniem standardowej dewiacji częstotliwości. Wartość BT równa 0,5 została wybrana uwzględniając dwa wymagania; efektywność wykorzystania pasma oraz zdolność do tolerowania interferencji międzysymbolowej. Dane binarne są odfiltrowane za pomocą wąskopasmowego filtru Gaussa (o szerokości pasma 500 kHz) z BT równym 0,5.

Zarówno 2-GFSK, jak i 4-GFSK posiadają tą samą średniokwadratową dewiację częstotliwości chwilowej o wartości sygnału nośnej. Dewiacje częstotliwości nośnych dla modulacji 2-GFSK i 4-GFSK przedstawiono w Tabeli 3.3, zaś schemat operacji związanych z wymienionymi modulacjami przedstawiono na rysunku 3.6.

Tabela 3.3. Dewiacja nośnej dla modulacji 2-GFSK i 4-GFSK

Modulacja	Dane	Dewiacja nośnej	Wskaźnik modulacji
2-GFSK	0	- 0,5 x h_2 x symbol rate	0,160
	1	+ 0,5 x h_2 x symbol rate	0,160
4-GFSK	00	- 1,5 x h_4 x symbol rate	0,216
	01*	- 0,5 x h_4 x symbol rate	0,072
	11	+ 0,5 x h_4 x symbol rate	0,072
	10*	+ 1,5 x h_4 x symbol rate	0,216

)* - najstarszy bit jest transmitowany jako pierwszy
h_2- maksymalna dewiacja względem częstotliwości środkowej dla 2-GFSK
h_4- maksymalna dewiacja względem częstotliwości środkowej dla 4-GFSK



Rys. 3.6. Wielopoziomowe modulacje GFSK

Każdy kanał FHSS zajmuje pasmo 1 MHz i musi realizować minimalną liczbę przeskoków, która jest określana przez różne ciała standaryzacyjne. Dla przykładu w USA określono minimalną wartość liczby skoków/sekundę jako równą 2,5, co odpowiada czasowi przebywania na danej częstotliwości równemu 400 ms. Czas trwania nadawania z zadaną częstotliwością może być modyfikowany przez stację pełniącą rolę punktu dostępowego AP w zależnie od stanu środowiska propagacyjnego. W standardzie 802.11 określono ilościowe wielkości związane z modelami FH optymalizując je pod kątem minimalizacji prawdopodobieństwa nadawania przez BSS na tej samej

częstotliwości i w tym samym czasie co inna BSS. W tabeli 3.4 przedstawiono zalecenia zawarte w standardzie 802.11 dotyczące minimalnej liczby częstotliwości kanałowych, bieżącej liczby częstotliwości kanałowych oraz wymaganej liczby wzorców.

Tabela 3.4. Wielkości charakteryzujące standard 802.11 FHSS związane z liczbą częstotliwości oraz harmonogramów skakania po częstotliwościach.

Region	Minimalna liczba kanałów częstotliwości	Bieżąca liczba kanałów częstotliwości	Liczba zbiorów harmonogramów przeskoków	Liczba harmonogramów przeskoków w każdym zbiorze	Liczba harmonogramów przeskakiwania po częstotliwościach
Europa	20	79	3	6	78
USA	75	79	3	26	78
Hiszpania	20	27	3	9	27
Francja	20	35	3	11	33
Japonia	10	23	3	4	12

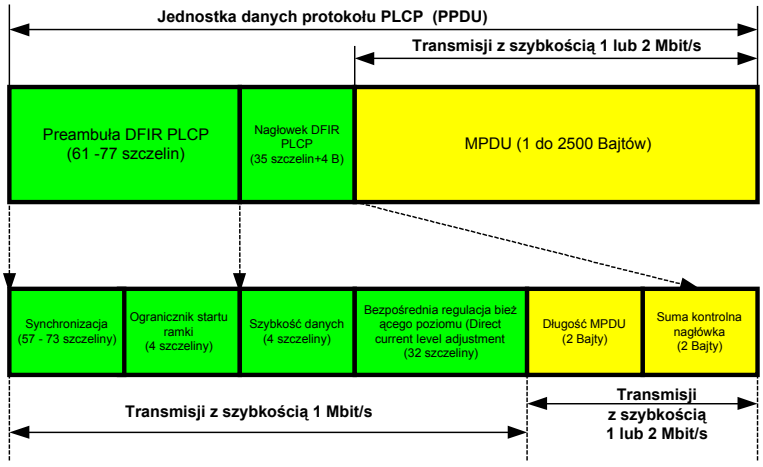
Minimalny odstęp w czasie przeskoków po paśmie zarówno w USA jak i w Europie (łącznie z Francją i Hiszpanią) wynosi 6 MHz natomiast w Japonii wynosi 5 MHz.

3.2.2.2 Warstwa fizyczna z wykorzystaniem fal optycznych podczerwieni

Warstw fizyczna zrealizowana za pomocą DFIR działa w zakresie podczerwieni o długości fali od 850 do 950 nm] stosując modulacje PPM (ang. *Pulse Position Modulation*) i nadając z mocą o wartości szczytowej równej 2 W. W ogólności system L-PPM będzie umieszczał fazę symbolu w L interwałach lub szczelinach czasowych.

Promieniowane wąskie impulsy w zakresie podczerwieni są transmitowane w jednym z przedziałów czasowych. Tak więc podobnie jak w modulacji wielopoziomowej, przepływność (szybkość) symbolowa może być mniejsza niż uzyskiwana przepływność. W odróżnieniu jednak od modulacji wielopoziomowej, pasmo w L-PPM wzrasta przez czynnik $L/\log_2 L$ względem intensywności modulacji "ON-OFF". Chociaż w szczelinach czasowych o krótszych interwałach może być przetransmitowana większa liczba bitów, węższe impulsy wymagają lepszego dopasowania do właściwych szczelin. Prowadzi to do wymagania użycia szerszego pasma, a więc wprowadzenia dodatkowego szumu, który ogranicza wydajność modulacji L-PPM.

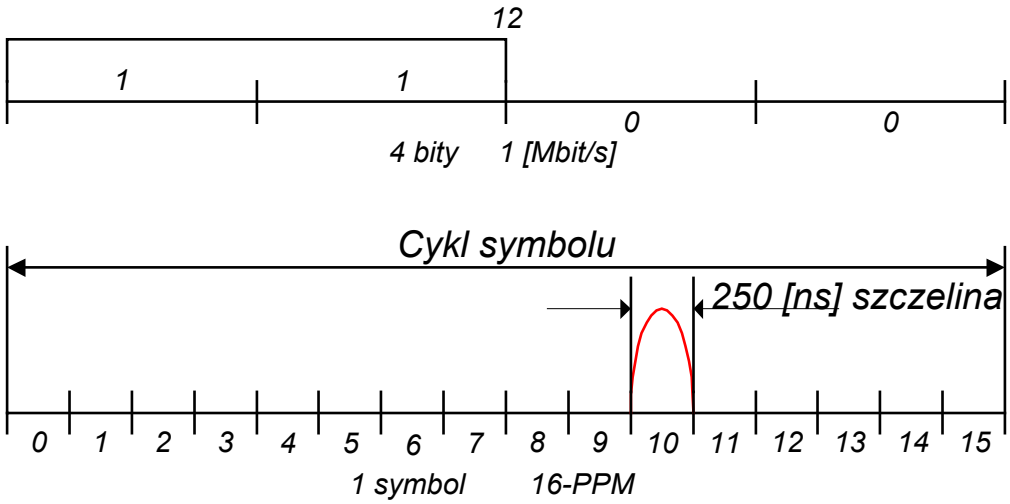
Format pakietu podwarstwy fizycznej DFIR 802.11 PLCP został przedstawiony na rysunku 3.7. Pierwsze trzy pola są transmitowane przy użyciu modulacji "*on - off keying intensity*"



Rys. 3.7. Format pakietu PLCP infrared LAN

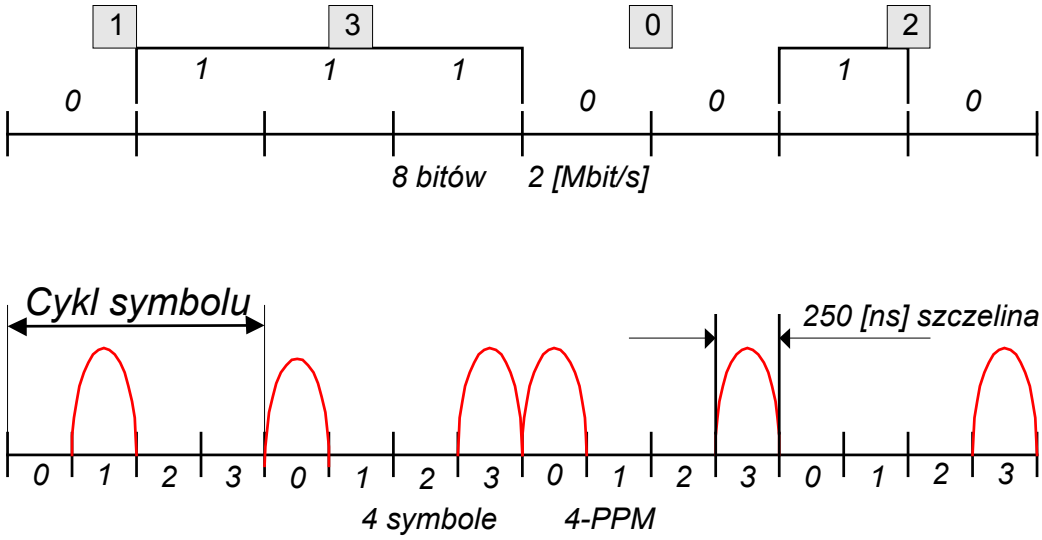
Do stabilizacji średniego poziomu sygnału odbieranego przez odbiornik (po odebraniu sygnałów pierwszych trzech pól) wykorzystuje się mechanizm bezpośredniej regulacji poziomu bieżącego - DCLA (ang. *Direct Current Level Adjustment*). Uruchomienie szablonu ogranicznika ramki SFD (ang. *Start Frame Delimiter*) wymaga rozważnego wyboru, ponieważ wpływa on bezpośrednio na PER (pakietową stopę błędów). Prawdopodobieństwo, że SFD zostanie poprawnie wykryty zależy od prawdopodobieństwa imitacji i prawdopodobieństwa błędu SFD. W standardzie 802.11 przyjęto wzór 1001, który jest jednym ze zbioru wzorców, który maksymalizuje prawdopodobieństwo wykrycia błędu w obszarze SFD. Przewidywane pola są transmitowane z zastosowaniem modulacji L-PPM.

Standard DFIR dla przepływności 1 Mbit/s stosuje 16 pozycyjną modulację PPM (16-PPM), w której 4 bity danych są odwzorowywane w od 1 do 16 impulsów, co zostało zobrazowane na rysunku 3.8.



Rys. 3.8. Modulacja sygnałów 16 - PPM 1 Mbit/s

Wersja 2 Mbit/s stosuje modulację 4-PPM gdzie 2 bity danych są odwzorowywane w od 1 do 4 impulsów (sygnałów), co zostało zobrazowane na rysunku 3.9.



Rys. 3.9. Modulacja 4-PPM sygnałów 2 Mbit/s

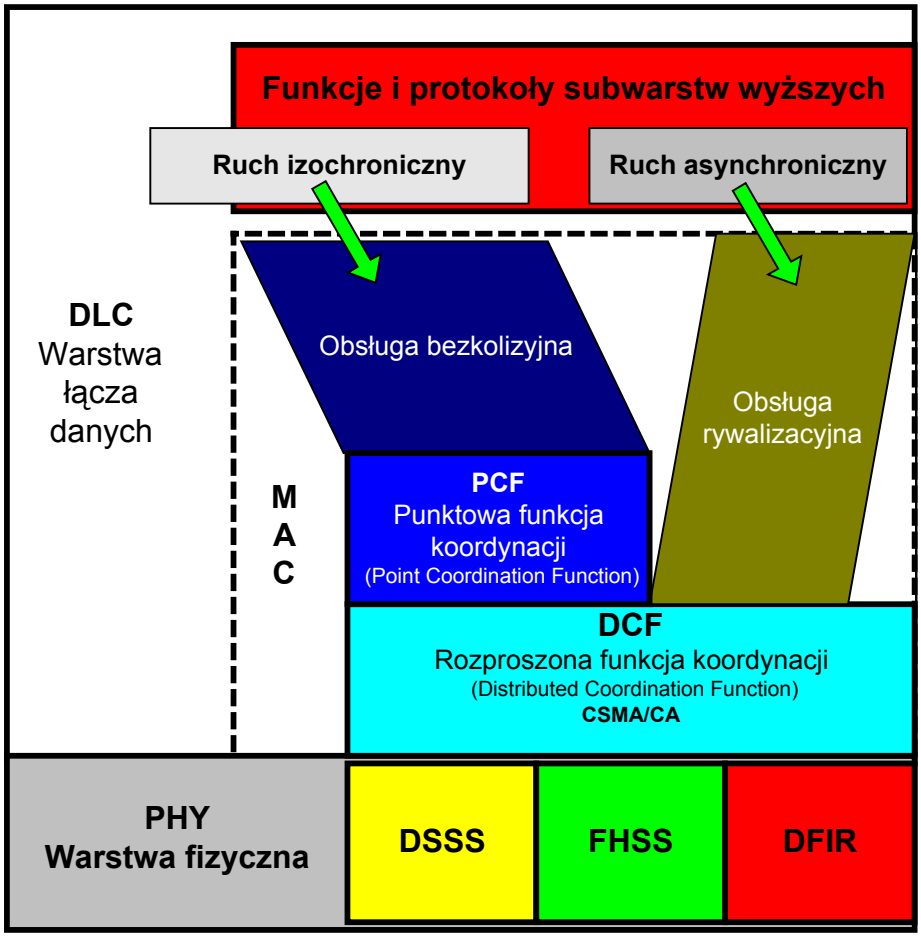
Tabela 3.5. Porównanie własności technk przesyłania sygnału w łączu fizycznym 802.11.

LP.	Rodzaj technologii / Parametry	DSSS	FHSS	DFIR
1.	**Przepływność Mbit/s**	2 - 20	1 - 3	1 - 4
2.	**Charakter stacji**	Stacjonarne/ruchome	Ruchome	Stacjonarne/ruchome
3.	**Zasięg w [m]**	30 -300	30 -100	10 -70
4.	**Zakres (częstotliwość/ dł. Fali)**			850 - 950 nm
5.	**Rodzaj modulacji**	DBPSK, QPSK	2,4-GFSK	L - PPM
6.	**Moc emitowana**	< 1 W	< 1 W	2 W
7.	**Metoda dostępu**	CSMA	CSMA	CSMA

3.2.3 Podwarstwa MAC standardu IEEE 802.11

W ramach specyfikacji podwarstwy MAC standardu IEEE 802.11 wyszczególniono pewne funkcje podstawowe oraz kilka funkcji opcjonalnych. Ich główne charakterystyki zostały skoncentrowane w regułach zapewniających dostęp do współdzielonego medium bezprzewodowego poprzez punkty dostępu do dwóch zasadniczych topologii sieci, tj. sieci stałych (z infrastrukturą) i tymczasowych (*ad-hoc*).

Interesującą własnością standardu 802.11 jest niezależność podwarstwy dostępu do medium niezależnie od sposobu realizacji warstwy fizycznej. Zatem funkcje protokołu MAC są wspólne dla wszystkich trzech opcji warstwy fizycznej (DSSS, FHSS, DFIR) i jest on niezależny od szybkości bitowej (przepływności). Zasadnicza część określająca zasady organizacji bezprzewodowych sieci LAN w standardzie 802.11 została zawarta w opisie określanym mianem DFWMAC (ang. *Distributed Foundation Wireless MAC*). W opisie tym zostały wyspecyfikowane funkcje i zasady pracy głównie podwarstwy MAC i dość ogólnie warstwy fizycznej. Ponieważ elementy warstwy fizycznej zostały omówione, pozostaje przedstawienie elementów podwarstwy MAC. Jej warstwowy model został przedstawiony na rysunku 3.10.



Rys. 3.10. Warstwowa architektura protokołu DFWMAC standardu 802.11

Protokół DFWMAC definiuje dwie wersje algorytmów pracy dla stacji i sieci. Wersje algorytmów związane są z dwoma rodzajami usług oferowanych przez podwarstwę MAC. Zarówno stacja jak i sieć może pracować w następujących trybach pracy:

1. Z rozproszoną funkcją koordynacji - DCF - stanowiący podstawowy tryb pracy;
2. Z punktową funkcją koordynacji - PCF - tryb przeznaczony wyłącznie dla sieci stałych wyposażonych w punkt dostępu

Pierwszy z wymienionych trybów jako metodę dostępu do medium wykorzystuje się protokół CSMA/CA[12], którego ogólna zasada działania polega na tym, że przed rozpoczęciem transmisji stacja musi sprawdzić stan medium. Jeżeli medium nie jest wykorzystywane przez określony czas, losowo wybrany zostaje moment czasu rozpoczęcia nadawania. Wartość losowego opóźnienia momentu nadawania T_{lo} (ang. *backoff*) wyliczana jest zgodnie z następującą zależnością:

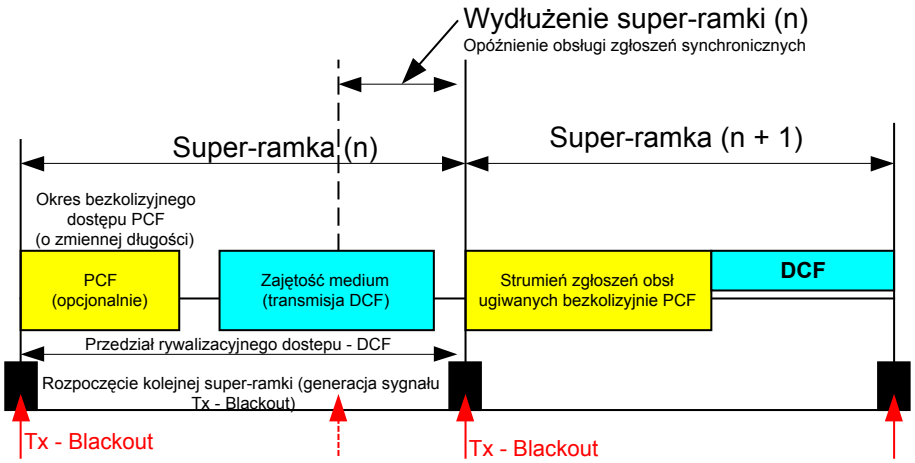
$$T_{lo} = \tau_{max} x\ \Delta t\ x\ Rd$$

gdzie:

- τ_{max}- maksymalna wartość opóźnienia w danej próbie dostępu do medium wyrażona liczbą szczelin czasowych;
- Δt - długość przedziału czasowego, który jest sumą opóźnienia propagacji sygnału w kanale, czasu przełączania nadajnika i czasu niezbędnego do wykrycia stanu zajętości kanału. Czas trwania szczeliny jest zależny od rodzaju rozwiązania przyjętego dla warstwy fizycznej;
- Rd - losowa liczba z przedziału <0,1>

[12] *Szczegółowy opis CSMA/CA został przedstawiony w dalszej części opracowania*

Tryb z punktową funkcją koordynacji PCF służy do obsługi ruchu izochronicznego oraz transmisji danych wrażliwych na ograniczenia czasowe. Mechanizmy koordynacji pracy stacji, niezbędne do zapewnienia okresowego dostępu do kanału, są zazwyczaj implementowane w punktach dostępu (AP) do infrastruktury sieci przewodowych. W przypadku realizacji trybu pracy kanału z punktową funkcją koordynacji PDF definiuje się tzw. "super-ramkę" czasową, w której wydzielone są części zarówno do transmisji wolnej od rywalizacji (bezkolizyjnej) jak i rywalizacyjnej zgodnej z trybem przyjętym w DCF. Organizacja super ramki została przedstawiona na rysunku 3.11.



Rys. 3.11. Organizacja "super ramki" standardu 802.11 w przypadku realizacji protokołu PCF

Długość "super-ramki" może podlegać niewielkim wahaniom, za przyczyną DCF, które zajmuje medium. Długość okresu bezkolizyjnego CFP (ang. *Contention Free Period*) waha się w zależności od liczby zgłoszeń.

Żądania bezkolizyjnej obsługi są realizowane przez stację punktu dostępowego za pomocą trybu DCF z wykorzystaniem rywalizacyjnej części super-ramki czasowej. Stacja AP wpisuje na listę stacje żądające tego typu usługi, które następnie są obsługiwane w bezkolizyjnym fragmencie super-ramki.

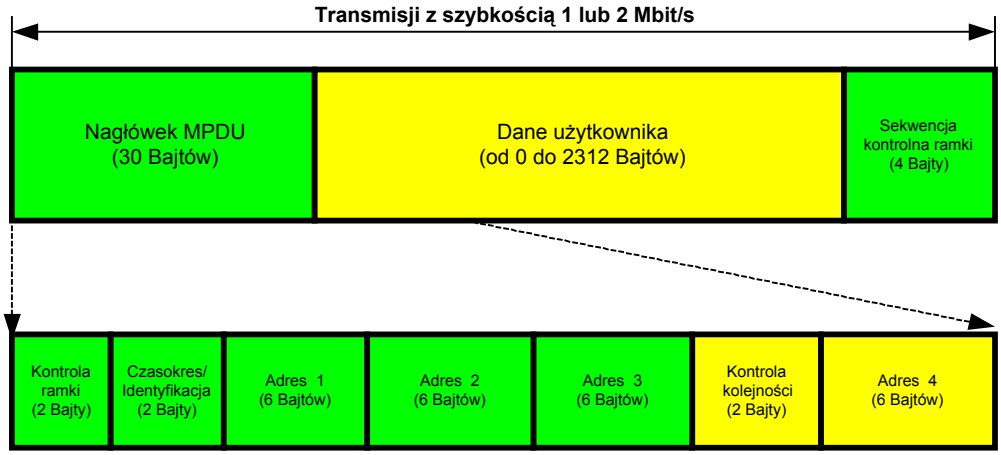
W ramach architektury protokołów DFWMAC podwarstwa MAC pełni szereg istotnych funkcji. Oprócz zapewniania usług transportowych podwarstwie LLC oraz sterowaniu dostępem do medium do zadań tej warstwy należy:

- Koordynacja pracy stacji, która jest bardzo istotna dla trybu pracy PCF;
- Nadzorowanie stacji w celu zapewnienia jej długotrwałej pracy i przedłużonej żywotności baterii akumulatorów. Przy pracy w sieci z infrastrukturą i realizacji funkcji PCF stacje pozostają przez większą część czasu pracy w stanie nieaktywnym (uśpienia), a punkty dostępu buforują wówczas kierowane do nich pakiety (ramki);
- Monitorowanie środowiska stacji w celu określenia pasma kanału fizycznego (w systemach wielokanałowych) oraz wyboru właściwego obszaru pracy stacji BSS[13] jak też związanej z tym obszarem punktu AP;
- Realizacja funkcji kontrolno sterujących pracą podwarstwy.

[13] *ang. Basic Service Set*

3.2.3.1 *Ogólna jednostka danych protokołu MAC 802.11*

Ogólny format jednostki danych protokołu MAC 802.11 (MPDU) został przedstawiony na rysunku 3.12.



Rys. 3.12. Ogólny format jednostki danych protokołu MAC 802.11 (MPDU)

Pola: Adres 2, Adres 3, Sekwencja sterująca, Adres 4 i Dane użytkownika są obecne tylko w określonych typach pakietów. MPDU jest oddzielnie zabezpieczany przez bity sprawdzające błędy. Występują trzy typy pakietów, a w tym:

- pakiety danych;
- pakiety sterujące (np. RTS (ang. *Request To Send*), CTS (ang. *Clear To Send*), pakiety potwierdzeń ACK (ang. *Acknowledge*);
- pakiety zarządzania (np. *Beacons*).

Informacje jakie są przenoszone w poszczególnych polach formatu nagłówka MPDU zostały wyszczególnione w tabeli 3.6.

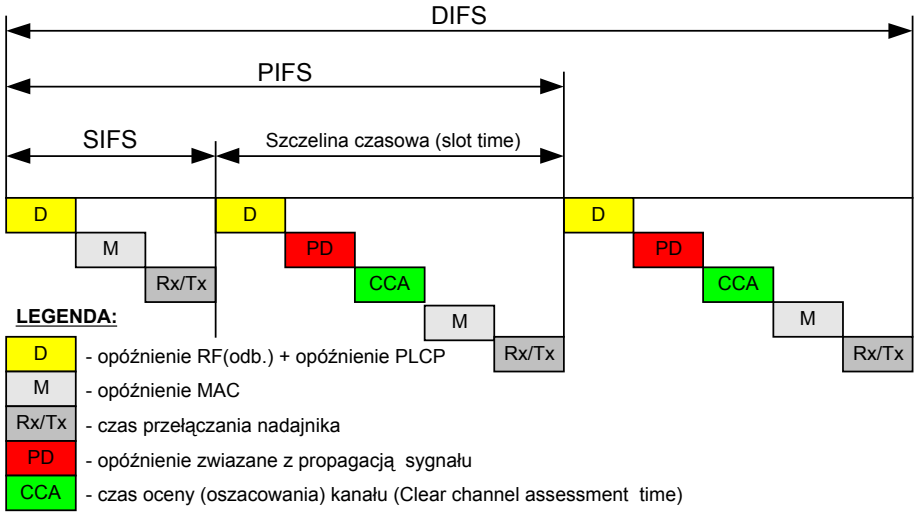
Tabela 3.6. Informacje przenoszone przez różne pola formatu nagłówka MPDU

LP.	Pole	Dostarczana informacja
1.	**Kontrola ramki** (*frame control*)	Bieżąca wersja standardu, odbierane pakiety lub przesłane do systemu dystrybucyjnego, zarządzanie mocą, fragmentacja pakietów, szyfrowanie i uwierzytelnianie (poświadczanie)
2.	**Czasokres/ identyfikacja** (*Duration/ identyfication*)	Czasokres alokacji wektora sieci, identyfikacja węzła działającego w trybie oszczędzania mocy
3.	**Adresy od 1 do 4**	Adresy dla BSS I, przeznaczenie, źródło, nadajnik i odbiornik
4.	**Kontrola kolejności** (*Sequence Control*)	Kolejny numer pakietu i fragmentu pakietu

3.2.3.2 *Przedziały czasowe - odstępy między ramkami*

W ramach protokołu podwarstwy MAC zostały zdefiniowane trzy istotne i różne przedziały czasowe - IFS (ang. *Interframe Space*). Przedstawione w formie graficznej na rysunku 3.13 przedziały czasowe są niezależne od wielkości przepływności w kanale bezprzewodowym. Służą do

określania czasu rozpoczęcia nadawania przez daną stację i są odmierzane przez każdą stację od chwili zakończenia zajętości medium.



Rys. 3.13. Definicje przedziałów czasowych MAC 802.11

Najmniejsza wartość przedziału czasowego - SIFS (ang. *short IFS*), nazywana krótkim przedziałem czasowym, jest wykorzystywana do wszystkich akcji wymagających bezpośrednich (natychmiastowych) odpowiedzi takich jak np. potwierdzenia transmisji ACK, pakietów RTS czy CTS.

Pośrednią długość IFS posiada przedział PIFS (ang. *Point Coordination Function IFS*), który jest używany wyboru węzła (stacji) zgodnie z wymaganymi ograniczeniami czasowymi. Najdłuższy z trzech wymienionych przedziałów czasowych - DIFS (ang. *Distributed Coordination Function IFS*) jest wykorzystywany jest do minimalizacji czasu opóźnienia pomiędzy kolejnymi pakietami danych. Zdefiniowana jest także szczelina czasowa (*slot time*), odpowiada ona szczelinie czasowej o losowej wartości odstępu między kolejnymi transmitowanymi pakietami, nazywanej *"backoff"* (zostanie omówiona przy omawianiu protokołów unikania kolizji). Przedział czasowy DISF jest sumą czasów; oceny kanału (wykrycia nośnej), przełączania nadajnika, opóźnienia związanego z propagacją sygnału oraz przetwarzaniem w podwarstwie MAC.

SIFS jest funkcją opóźnienia w odbiorniku, dekodowania preambuły /nagłówka w podwarstwie PHY niezależnej od medium - PLCP, czasu przełączania nadajnika i opóźnienia związanego z przetwarzaniem w podwarstwie MAC.

W standardzie 802.11 zdefiniowano różne wartości dla szczelin czasowych i SIFS dla różnych warstw fizycznych. I tak dla przykładu w sieciach LAN z DSSS określono wartość dla SIFS = 10 μs i szczelinę (slot) = 20 μs. Z kolei dla sieci LAN z FHSS wartości te wynoszą: SIFS = 28 μs i szczelina = 50 μs. DIFS jest zdefiniowany jako SIFS + 2 x szczelina, gdzie PIFS jest określone jako SIFS + szczelina czasowa. Pozostałe szczegółowe wartości zostały przedstawione w tabeli:

Tabela 3.7. Szczeliny czasowe dla różnych typów odstępów i warstw fizycznych standardu 802.11

LP.	Rodzaj odstępu miedzy ramkami	DSSS [μs].	FHSS [μs].	DFIR [μs].
1.	SIFS	10	28	7
2.	PIFS	30	78	15
3.	DIFS	50	128	23
4.	Szczelina (slot)	20	50	8

Dokonując porównania owych wartości można zauważyć, że przedziały czasowe - IFS, dla systemu DSSS są najmniej dwa razy krótsze niż dla systemu FHSS. Oznacza to, że transmisja DSSS wykorzystuje mniejszą część nagłówkową w porównaniu do szczeliny miedzy ramkami. Przy okazji można zaznaczyć, że szczelina czasowa (slot) dla Ethernetu 10 Mbit/s jest zdefiniowana jako 512 bitów lub 51,2 μs.

3.2.4 Rozproszona funkcja koordynacji DCF

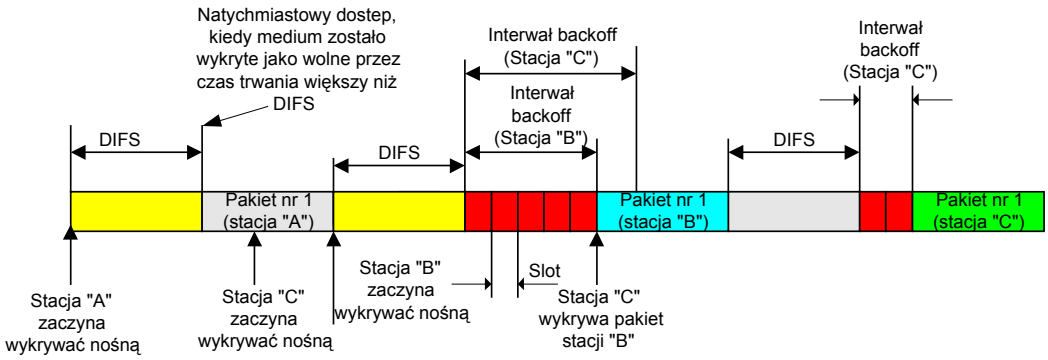
Podstawowa metoda dostępu do łącza w standardzie 802.11 została nazwana trybem z rozproszoną funkcją koordynacji - DCF (ang. *Distributed Coordination Function*). Jest to metoda dostępu do medium zasadniczo oparta o algorytm rywalizacyjnego dostępu z unikaniem kolizji - CSMA/CA (ang. *Carrier Sense Multiple Access with Collision Avoidance*).

Algorytm CSMA/CA jest bardzo podobny do algorytmu rywalizacyjnego dostępu z wczesnym wykrywaniem kolizji - CSMA/CD (ang. *Carrier Sense Multiple Access with Collision Detection*) stosowanym w przewodowych sieciach Ethernet. Oba wymienione typy protokołów dostępność do transmisji w medium wykrywają poprzez śledzenie i wykrywanie nośnej. Ubieganie się o dostęp do medium jest rozstrzygane przy wykorzystaniu eksponencjalnego algorytmu z losowym odstępem między ramkami (*backoff*). Protokół CSMA/CA wykorzystuje sterowanie rozproszone w przeciwieństwie do zcentralizowanego sterowania dostępem stosowanego w przewodowych sieciach LAN. Zatem stacja może transmitować, "kiedy sobie życzy" i tak długo jak przestrzega reguł protokołu.

W CSMA, stacja która ma pakiet do transmisji najpierw sprawdza stan łącza, a w wypadku jego zajętości prze inne stacje wstrzymuje się z transmisją i ewentualnie czeka na zwolnienie kanału. Jeżeli na podstawie informacji pomocniczych o stanie kanału poprzez śledzenie nośnej stwierdza, że kanał jest wolny przez okres czasu dłuższy niż DIFS pakiet jest transmitowany w trybie natychmiastowym. Podwarstwa MAC działa w połączeniu z warstwą fizyczną oszacowując stan medium. Metoda ta pozwala na pomiar poziomu sygnału radiowego w celu określenia poziomu wzmocnienia odbieranego sygnału. Jeżeli odbierany sygnał znajduje się poniżej określonego progu, medium jest zadeklarowane jako do oceny i podwarstwa MAC nadaje status dla transmisji pakietów jako stan oceny kanału CCA (ang. *Clear Channel Assessment*). Inną metodą korelacji odbieranego sygnału z 11- bitowym (chip) kodem Barker'a wykrywa obecność właściwego sygnału DSSS. Obie metody mogą być zastosowane jako kombinacja w celu zapewnienia większej niezawodności poprawnego oceniania bieżącego statusu medium.

3.2.4.1 Unikanie kolizji

Protokół CSMA z unikaniem kolizji (CA) wprowadza losowe odstępy między kolejno transmitowanymi pakietami. Unikanie kolizji jest wymagane w celu redukcji wysokiego prawdopodobieństwa kolizji natychmiast po pomyślnej transmisji pakietu. Zasadniczo jest to próba separacji całkowitej liczby transmitujących stacji w mniejsze grupy, z których każda używa różnych długości szczelin czasowych (znanych jako ang. *backoff time slot*). Jeżeli medium jest wykryte jako zajęte stacja musi po pierwsze opóźnić nadawanie do czasu zakończenia interwału czasu - DIFS i dalej czekać na losową liczbę określającą przedział czasu oczekiwania (nazywanej interwałem "backoff") zanim podejmie próbę transmisji. Opisana sytuacja została zobrazowana na rysunku:



Rys. 3.14. Transmisja pojedynczego pakietu z użyciem protokołu CSMA/CA

3.2.4.2 Wykrywanie kolizji i wykrywanie błędów

Mechanizm wykrywania kolizji wykorzystywany w przewodowych sieciach LAN wymaga od odbiornika ciągłego śledzenia transmisji w medium i wykrywania, kiedy realizowana jest w nim transmisja. Tego typu mechanizmy nie mogą być bezpośrednio wykorzystane w sieciach bezprzewodowej z kilku powodów. Po pierwsze w sieciach przewodowych różnice pomiędzy poziomami sygnałów nadawczych i odbiorczych (dynamika sygnału) jest mała i umożliwia łatwe wykrywanie kolizji.

W środowisku bezprzewodowym emitowana energia sygnału jest promieniowana we wszystkich kierunkach i odbiorniki muszą charakteryzować się bardzo dużą czułością, żeby odebrać sygnał. Nie bez znaczenia jest fakt, że odbiornik znajduje się w bezpośredniej bliskości nadajnika. Powoduje to, że kiedy dwa lub więcej węzłów nadaje w tym samym czasie występujące kolizje będą trudno wykrywalne, ponieważ poziom transmisji sygnału od wysyłającego węzła przekracza poziom transmisji sygnałów od innych węzłów. Co więcej, podstawowym założeniem dla wykrywania kolizji jest to żeby wszystkie węzły były w zdolne "słyszeć" siebie nawzajem. Tego typu wymaganie jest mało praktyczne w środowisku bezprzewodowym, ponieważ mocno osłabiony i zmienny sygnał czyni wykrywanie kolidujących ze sobą pakietów jako trudne. Sytuację pogarsza zjawisko "stacji ukrytej".

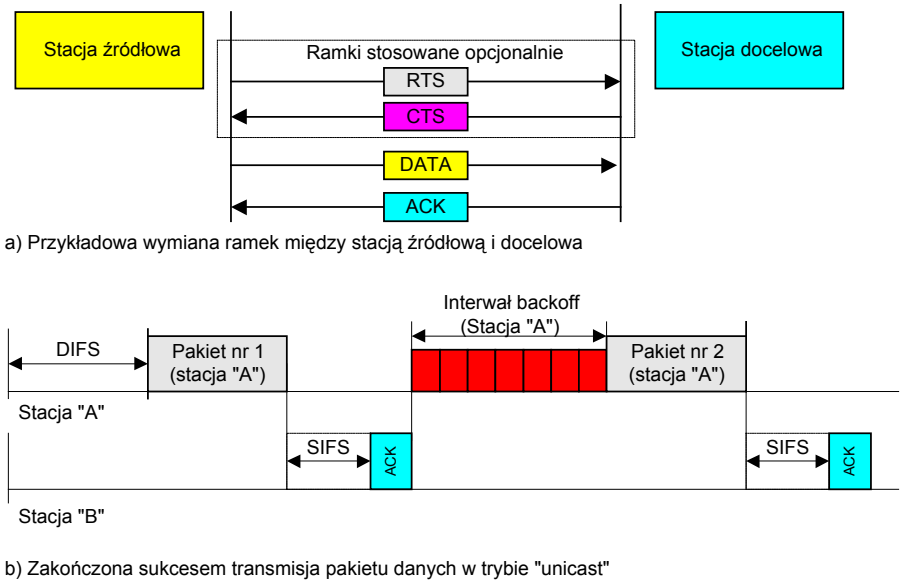
Zjawisko stacji ukrytej występuje, kiedy nie wszystkie stacje mają bezpośrednią łączność. Stacja jest "ukryta", jeżeli znajduje się w zasięgu stacji odbierającej dane, ale jest poza zasięgiem stacji nadającej. Stacja "A" nadaje do stacji "B". Ponieważ stacje "A" i "C" znajdują się poza swoim zasięgiem transmisja nie zostanie wykryta w stacji "C". Stacja "C" przyjmuje, że łącze jest wolne i może rozpocząć transmisję do stacji "B" lub "D". Transmisja ta powoduje w stacji "B" kolizję z danymi ze stacji "A". Taka sytuacja powoduje z kolei spadek przepustowości łącza w skutek konieczności częstych retransmisji.

W końcowym efekcie wykrywanie kolizji wymaga dwukierunkowych i kosztownych implementacji tj. pełno dupleksowy radionadajnik pozwalający na nadawanie i odbiór w tym samym czasie.

W sieciach WLAN zastosowano rozbudowany algorytm CSMA, który został nazywany protokołem dostępu CSMA/CA. Protokół ten stanowi odmianę protokołu CSMA bądź CSMA/CD (IEEE 802.3), którego elementy ze względu na wspomniane powyżej wady, uniemożliwiają jego zastosowanie w kanałach radiowych. Protokół dostępu CSMA/CA posiada szereg nowych elementów, do których należą:

- zróżnicowane czasy opóźnień (w podejmowaniu różnych działań protokolarnych), dostosowane do priorytetów przesyłanych wiadomości;
- specjalne pakiety (ramki) sterujące: RTS (ang. *Request To Send*) i CTS (ang. *Clear To Stnd*), pozwalające na wstępną rezerwację medium i szybsze rozwiązywanie ewentualnych kolizji;
- liczniki czasu wyznaczające narzucone protokołem DFW działania stacji.

W omawianym standardzie (protokół 802.11 MAC) zakłada się, że wszystkie jednoadresowe ramki DATA muszą być powiadamiane pozytywnie ramkami ACK (ang. *acknowledgement*), oczywiście, jeżeli pakiet został odebrany poprawnie. Również ramki RTS wymagają potwierdzenia ramkami CTS. Zostało to zilustrowane w części a) rysunku 3.15.



Rys. 3.15. Wymiany ramek między stacją źródłową i docelową (a) oraz potwierdzana transmisja pakietów danych w trybie "punkt-punkt"

Ramki RTS i CTS są szczególnie użyteczne w sytuacjach, gdy:

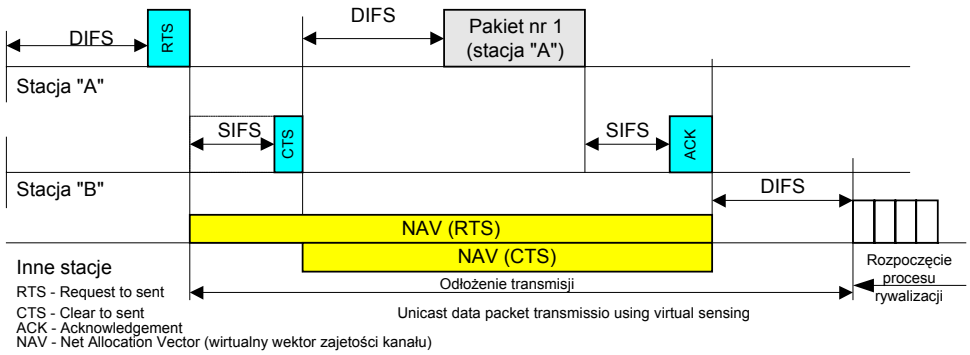
- istnieje potrzeba przesyłania długich pakietów DATA, bądź też;
- w sieci mamy do czynienia z tzw. stacjami ukrytymi, tj. znajdującymi się poza zasięgiem bezpośredniej słyszalności stacji (sieć z transmisją wieloetapową). Istnienie stacji ukrytych (ang. *hidden stations*) w sposób istotny obniża efektywność algorytmów CSMA. Niekorzystny wpływ stacji ukrytych na jakość protokołu DSMA może być znacznie ograniczony poprzez zastosowanie algorytmu DCF z opcjonalnym wykorzystaniem ramek (pakietów) RTS/CTS.

Potwierdzenie ACK jest transmitowane zawsze po szczelinie SIFS, która każdorazowo trwa krócej niż DIFS co pozwala na transmitowanie ramek ACK przed każdym nowym pakietem. (rysunek 3.15b). W sytuacji kiedy nie zostanie otrzymane potwierdzenie ramki, nadajnik zakłada, że pakiet jest zagubiony/ niepoprawny (np. wystąpiła kolizja lub błąd transmisji) i retransmituje pakiet. Retransmisja jest realizowana przez podwarstwę MAC a nie przez wyższe warstwy, co stanowi niewątpliwą zaletę tego rozwiązania.

W bezprzewodowych sieciach LAN błędy odbioru występują częściej niż w przewodowych sieciach LAN. Zastosowanie potwierdzeń ACK zmniejsza efektywną szybkość transmisji, ale jest nieodzowne w kanałach radiowych. Potwierdzanie ACK jest wymagane jedynie dla wymiany typu "punkt - punkt". Potwierdzenie dla ruchu rozgłoszeniowego i wielopunktowego nie jest wymagane, gdyż jest uznawane jako mało efektywne (np. z powodu częstego występowania kolizji potwierdzeń).

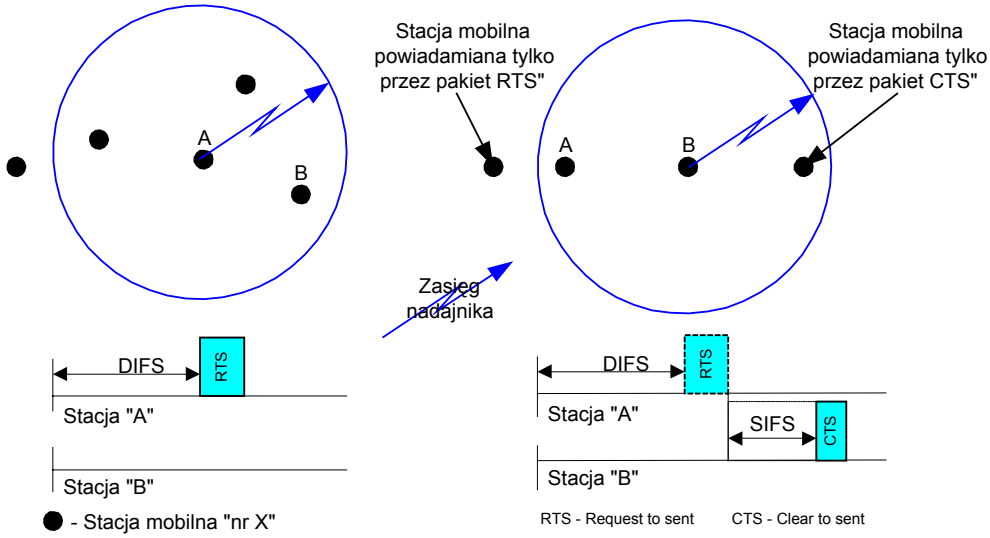
3.2.4.3 Wirtualne wykrywanie

Protokół CSMA/CA - może być rozszerzony poprzez włączenie wirtualnego mechanizmu wykrywania nośnej, który dostarcza informacje związanej z rezerwacją poprzez ogłaszanie zapowiedzi o zbliżającej się możliwości wykorzystaniu medium bezprzewodowego. Realizacja tej funkcji odbywa się przez wymianę krótkich pakietów sterujących nazywanych RTS i CTS (por. powyżej). Pakiety RTS są wysyłane przez stację nadającą, podczas gdy pakiety CTS są wysyłane przez stację odbiorcy przyznając stacji żądającej pozwolenie na transmisję. (rysunek 3.16).



Rys. 3.16. Transmisja pakietu typu punkt-punkt z wykorzystaniem wirtualnego wektora zajętości kanału

Pakiety RTS i CTS zawierają pola, które definiują okres czasu rezerwacji medium dla transmisji pakietu danych i pakietu ACK. Pakiety RTS i CTS minimalizują występowanie stanów kolizyjnych i pozwalają także stacji nadającej na szybkie ocenianie przypadków występowania kolizji. Dodatkowo, pakiet CTS alarmuje sąsiednie stacje (te, które znajdują się w jej zasięgu odbiorczym a nie nadawczym), aby powstrzymały się z nadawaniem pakietów do tej stacji, w ten sposób redukując kolizje związane z występowaniem zjawiska stacji ukrytej. Opisana sytuacja została zobrazowana na rysunku 3.17 (a).



Rys. 3.17. a) Transmisja pakietów RTS, b) Transmisja pakietów CTS

W ten sam sposób pakiet RTS zabezpiecza obszar transmisji przed kolizją, kiedy pakiet ACK jest wysyłany od stacji odbiorczej. Zatem, informacje związane z rezerwacją są dystrybuowane dookólnie. Wszystkie inne stacje, które poprawnie zdekodują pola informacyjne pakietów RTS i CTS zapamiętają informacje o rezerwacji medium w wirtualnym wektorze alokacji sieci NAV (ang. *Net Allocation Vector*). Dla tych stacji, NAV jest stosowany w połączeniu z wykrywaniem nośnej określającą dostępność medium. Stacje, których NAV nie ma wartości zerowej lub stan nośnej wskazuje na ich zajętość będą powstrzymywać się od nadawania.

Podobnie jak mechanizm potwierdzania ACK, rozpoznawanie wirtualne nie jest stosowane dla MPDU z adres rozsiewczym lub rozgłoszeniowym, z powodu prawdopodobieństwa kolizji ze względu na dużą liczbę pakietów CTS. Stąd, standard 802.11 pozwala na transmisje tylko krótkich pakietów bez wirtualnego wykrywania. Kontrola realizowana jest za pomocą parametru nazywanego "próg RTS". Tylko pakiety o długości większej niż próg RTS są transmitowane z wykorzystaniem mechanizmu wirtualnego wykrywania (NAV). Należy zauważyć, że efektywność algorytm wirtualnego wykrywania silnie zależy od przyjęcia założenia, że obie stacje nadawcza i odbiorcza, posiadają podobne parametry techniczne (np. moc nadawania i czułość odbiornika). Stosowanie mechanizmu wirtualnego wykrywania jest opcjonalne, lecz musi on być implementowany.

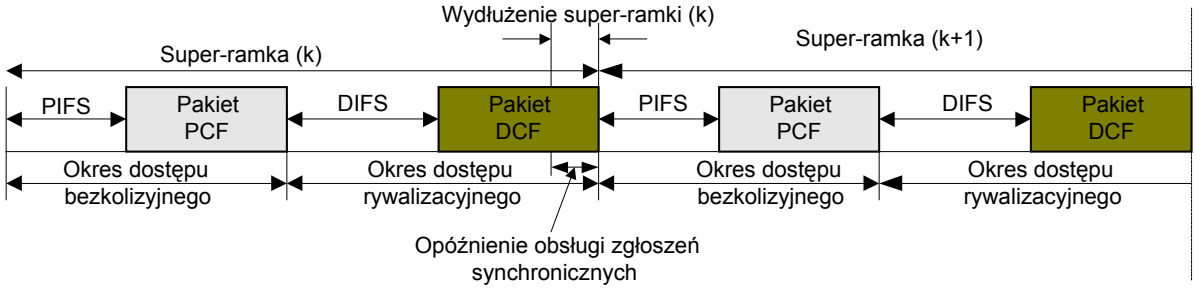
3.2.4.4 *Tryb z punktową funkcją koordynacji (dostępu)*

Ruch usług wrażliwych czasowo, wymaga skończonej wartości opóźnienia poza przekroczeniu, której przesyłana informacja jest pozbawiona wartości i może być odrzucona. Wymagania te wyraźnie kontrastują z wymaganiami dotyczącymi opóźnień dla ruchu danych. Dla tego typu ruchu ograniczenia w tym względzie są niższe.

CSMA/CA nie jest szczególnie predysponowany do zabezpieczenia ruchu usług wrażliwych czasowo, ponieważ traktuje wszystkie pakiety jednakowo i jako pakiety danych. Jest to cechą systemu bezpołączeniowego, nie szereguje lub nie nadaje priorytetów pakietom przenoszącym ruch wrażliwy czasowo (głos, wideo) i jako rezultat nie jest w stanie rozróżniać pomiędzy ruchem czasu rzeczywistego a ruchem nie wrażliwym czasowo (dane). Możliwość kolizji, losowy czas oczekiwań (backoff) oraz transmisje długich pakietów mogą powodować zmienność opóźnień (jitter). Podobnie jak ACK dla kolizji i wykrywanie błędów CSMA/CA może zniekształcać transmisję ruchu czasu rzeczywistego poprzez wzrost opóźnienia spowodowanego przez retransmisje.

Do eliminacji tego typu wad dla ruchu czasu rzeczywistego, jako opcja może być zastosowana funkcja punktowej koordynacji dostępu PCF. PCF stosuje, zdecentralizowany, bezkolizyjny wielopunktowy schemat dostępu, kiedy stacje są dopuszczone i posiadają zezwolenie na transmisję wydane przez punkt dostępowy AP. Należy zauważyć, że kolizje mogą występować w czasie AP transmituje wiadomości z zapytaniem do stacji mobilnych znajdujących się w obszarze zasięgu (pokrycia). Taka sytuacja pozwala innym węzłom chcących transmitować dane w trybie asynchronicznym na dostęp do medium.

Protokół MAC zmienia tryby pracy między DCF i PCF, lecz wyższy priorytet dostępu ma PCF. Pozwala to na zastosowanie koncepcji super-ramki, gdzie PCF jest aktywne w okresie bez rywalizacji.



Rys. 3.18 Współistnienie PCF i DCF w super-ramce

4 Bluetooth

Wszelkie urządzenia przenośne zyskują coraz większą popularność. Ich znaczenie wzrosło zwłaszcza wraz pojawianiem się takich urządzeń, jak komputery typu laptop czy palmtop, które pozwalają na wygodne wykorzystywanie pojedynczego urządzenia zarówno w pracy jak i w domu.

W tym kontekście istotnym problemem jest dogodny sposób łączenia różnych urządzeń przenośnych, bowiem wykorzystanie przewodu eliminuje walory mobilności. Popularny sposób łączenia z użyciem podczerwieni ma wiele ograniczeń, takich jak choćby konieczność optycznej widoczności obu urządzeń, stąd pojawienie się dowolnej przeszkody uniemożliwia lub w poważnym stopniu zakłóca transmisję. Innym częstym ograniczeniem jest konieczność konfigurowania mających współpracować urządzeń. Radykalnym sposobem na wyeliminowanie wspomnianych problemów jest zastosowanie fal radiowych. Rozwiązania tego typu i zastosowanie odpowiednich procedur umożliwiają stosunkowo łatwe komunikowanie się wielu urządzeń jednocześnie bez udziału użytkownika. Stanowi to o dużej atrakcyjności i użyteczności rozwiązania.

Kolejnym standardem pozwalającym na komunikację urządzeń przy użyciu fal radiowych jest system Bluetooth, którego początek datuje się na 1994 rok. Wtedy to firma Ericsson Mobile Communications rozpoczęła badania mające na celu opracowanie metody, która pozwoli zastąpić połączenia kablowe i bezprzewodowe optyczne, łączące telefony komórkowe z urządzeniami peryferyjnymi. W 1998 roku powstała grupa tematyczna Bluetooth SIG, w której skład wchodziły następujące firmy: Ericsson Mobile Communications AB, Intel Corp., IBM Corporation, Nokia Mobile Phones, Toshiba Corporation. Do grupy Bluetooth SIG dołączały kolejne znaczące korporacje, takie jak choćby Microsoft, Lucent, 3Com, Motorola. W niedługim czasie w składzie grupy Bluetooth SIG znalazło się około 1800 firm, pojawiła się też formalna specyfikacja protokołu (Bluetooth v. 1.0).

Wypracowanie satysfakcjonujących rozwiązań normatywnych nie było łatwe ponieważ podstawowy standard Bluetooth oraz jego rozwojowe wersje, aby spełnić pokładane w nim nadzieje, muszą zapewnić realizację następujących wymagań: ekstremalnie niskie koszty, mała moc nadajników (niewielki zasięg jest w tym przypadku zaletą) i otwartość systemu w znaczeniu modelu OSI/ISO, tzn. od radiowej warstwy fizycznej do poziomu aplikacji. Ponieważ omawiany standard przeznaczony jest dla urządzeń przenośnych (telefony komórkowe, komputery typu laptop itp.), istnieje konieczność zachowania małych gabarytów oraz niskiej masy urządzeń, a także uwzględnienie określonych uwarunkowań związanych z zasilaniem bateryjnym. Wymagany jest skrajnie niski pobór mocy i konieczność funkcjonowania urządzeń przy niskich napięciach zasilania. Wspomniane wymagania nie mogą równocześnie powodować zmniejszenia niezawodności i prostoty użytkowania urządzeń. Powszechność i dostępność standardu wymusza konieczność kompatybilnej współpracy urządzeń pochodzących od wielu różnych producentów.

4.1 Warstwa fizyczna protokołu Bluetooth

Urządzenia Bluetooth działają w powszechnie dostępnym, niewymagającym licencji paśmie przeznaczonym dla celów przemysłowych, naukowych i medycznych, znany jako ISM. Obostrzenia związane z wykorzystaniem zakresu, warunki emisji i interferencji zostały określone przez specyfikacje ETSI (ETS 300 – 328) w Europie i FCC (CFR47 Part 15) w USA. W niektórych krajach, na przykład we Francji, pasmo to podlega pewnym ograniczeniom, ale najprawdopodobniej w niedalekiej przyszłości zostanie udostępnione w całym zakresie.

Pasmo ISM jest wykorzystywane przez wiele urządzeń, takich jak różnego rodzaju urządzenia antywłamaniowe, bezprzewodowe słuchawki i telefony oraz omawiane sieci WLAN. Równocześnie stanowi ono zasób niechroniony, co sprawia, że występują w nim liczne zakłócenia generowane przez urządzenia powszechnego użytku (kuchenki mikrofalowe, lampy sodowe itp.). Zaletą użycia ISM jest jego powszechna dostępność, zapewniająca możliwość działania urządzeń Bluetooth na całym świecie.

W celu zapewnienia niezawodnej pracy urządzeń Bluetooth stosowane są techniki podobne jak we wcześniej opisanych sieciach WLAN. Należą do nich częste zmiany wykorzystywanej częstotliwości, adaptacyjne sterowanie mocą nadajnika sygnału i odpowiedni dobór długości pakietów danych.

Jako podstawowy schemat nadawania wykorzystywana jest technika przeskoków częstotliwości FHSS (*ang. frequency hopping*). Zapewnia ona na bezpieczną i niezawodną komunikację w przypadku występowania różnego rodzaju zakłóceń, co w paśmie ISM jest bardzo prawdopodobne. Uwzględniono również inne rozwiązania np. mechanizm retransmisji utraconych pakietów na innej częstotliwości niż transmisja pierwotna. W celu minimalizacji prawdopodobieństwa kolizji między pakietami własnej, niewielkiej obszarowo sieci zwanej pikosiecią i emisjami generowanymi w sąsiednich pikosieciach, w standardzie Bluetooth na poziomie fizycznym zastosowano specjalny algorytm. Algorytm ten dobiera odpowiednie częstotliwości uwzględniając funkcjonowanie innych pikosieci i następnie wyznacza sekwencję skoków z odpowiednio bezpiecznymi odstępami między wykorzystywanymi kanałami.

W dostępnym paśmie wydzielanych jest (w zależności od państwa) od 26 do 79 kanałów o szerokości 1 MHz i przepustowości Mbit/s. Stosowaną modulacją jest GFSK (*ang. Gaussian Frequency Shift Keying*). Standard Bluetooth przewiduje wykorzystanie multipleksowanie w dziedzinie czasu TDM (*ang. Time Division Multiplexed*), gdzie szczelina czasowa trwa 625 μs. W przypadku operacji poprzedzających transmisję (wykrywanie dostępnych urządzeń, wywołanie określonego terminala w celu nawiązania z nim połączenia) mogą być stosowane szczeliny czasowe o długości równej połowie zwykłej szczeliny czasowej. Generalnie, w ramach standardu na poziomie warstwy fizycznej (radiowej) zdefiniowano klasy urządzeń, uwzględniając dysponowaną moc nadawania i osiągany zasięg. Klasyfikację tą zawarto w tablicy 4.1.

Tabela 4.1. Klasy urządzeń standardu Bluetooth ze względu na moc nadawania i uśredniony zasięg

LP	KLASA URZĄDZENIA	MOC [dBm]	MOC [mW]	ZASIĘG [m]
1.	1	20	100	100
2.	2	4	2,5	10
3.	3	0	1	0,1

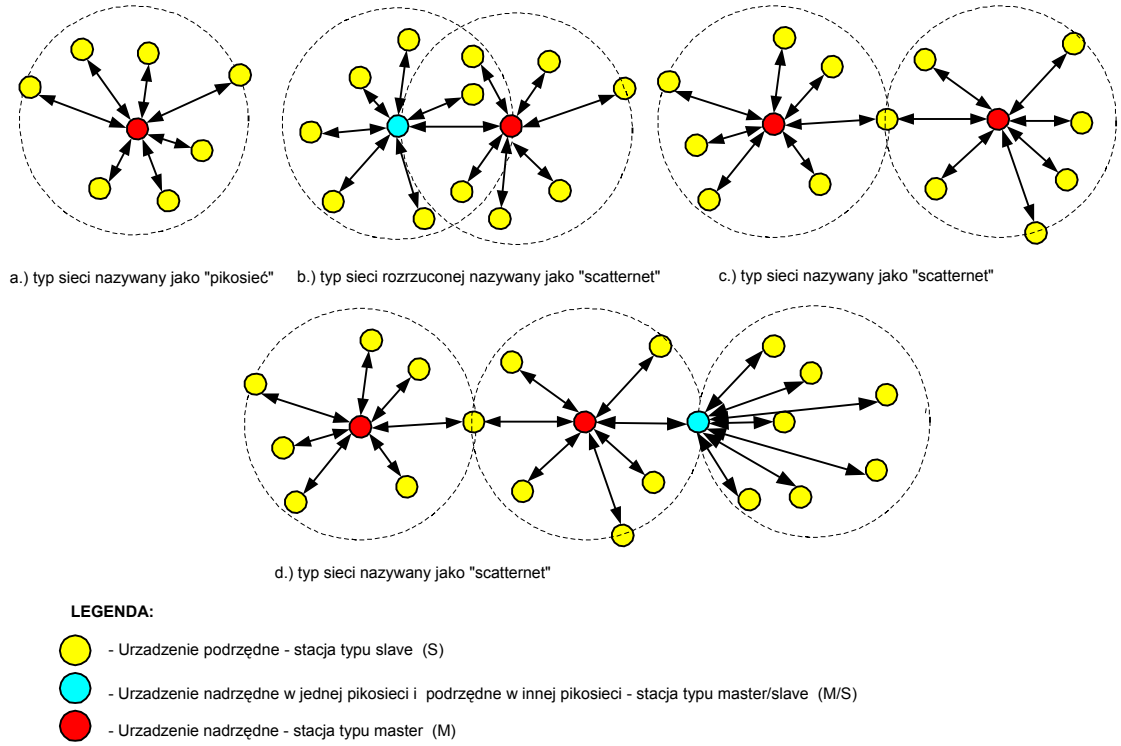
4.2 Urządzenie nadrzędne, podrzędne

Urządzenie Bluetooth może pracować w dwóch trybach: jako urządzenie nadrzędne (M), (*ang. master*) lub jako urządzenie podrzędne (S), (*ang. slave*). Sekwencję skoków częstotliwości określa urządzenie nadrzędne. Urządzenia podrzędne synchronizują się czasowo i częstotliwościowo do urządzeń nadrzędnych, powtarzając ich sekwencję skoków.

Każde urządzenie Bluetooth ma unikatowy adres i własny zegar. Adres ten i wartość okresu zegara są przekazywane podczas nawiązywania połączenia i na tej podstawie jest wyznaczana sekwencja skoków częstotliwościowych wykorzystywana podczas transmisji. Ponieważ wszystkie urządzenia podrzędne działające w ramach jednej sieci o niewielkich rozmiarach (pikosieci) pracują wykorzystując zegar i adres urządzenia nadrzędnego, każde z nich jest zsynchronizowane z urządzeniem nadrzędnym. Urządzenie nadrzędne określa także, momenty czasowe, w których dane urządzenie podrzędne może nadawać. Realizuje to poprzez przydział szczelin czasowych obsługiwanym terminalom, w zależności od typu przesyłanych danych. Przydział szczelin czasowych uwzględnia tryb transmisji (asynchroniczny, synchroniczny) oraz przepływność wymaganą dla realizacji usługi. I tak np. dane przesyłane są w trybie transmisji asynchronicznej natomiast głos przesyłany jest jako przekaz synchroniczny.

4.3 Rodzaje stosowanych sieci

Na rysunku przedstawiono dwa zasadnicze typy sieci występujące w systemie Bluetooth. Pierwszy z nich, przedstawiony na rysunku 4.1(a) nazwany został pikosiecią. W sieci tego typu występują dwa rodzaje urządzeń funkcjonalnych. Są to jednostki podrzędne (S) oraz element nadrzędny (M). Wszystkie urządzenia podrzędne pikosieci komunikują się z jednym urządzeniem nadrzędnym wykorzystując pojedynczą sekwencję skoków częstotliwościowych i takt zegarowy. Oznacza to, ze między urządzeniami podrzędnymi nie występują połączenia bezpośrednie. Liczba urządzeń podrzędnych komunikujących się za pośrednictwem współużytkowanego elementu nadrzędnego jest w jednej pikosieci ograniczona do siedmiu[14].



Rys. 4.1. Typy struktur sieci w standardzie Bluetooth

Urządzenie w sieci Bluetooth może korzystać z następujących typów adresów:

- Adres urządzenia (unikatowy) w postaci 48 bitów - ang. *Bluetooth Device Address*;
- Adres urządzenia aktywnego w połączeniu (3 bity)- ang. *Active Member Address*;
- Adres urządzenia nieaktywnego (8 bitów) - ang. *Parked Member Address*;
- Unikatowy adres nieaktywnego urządzenia używany podczas ustalania, w której szczelinie może wysyłać żądanie przejścia w stan aktywny - ang. *Access Request Address*.

Każde urządzenie przyłączone do pikosieci posiada adres typu AMA lub PMA. Adresy są ważne tak długo, jak długo urządzenie przebywa w stanie aktywnym/pasywnym.

Drugi typ sieci zobrazowany na rysunkach 4.1 b oraz c, stanowi złożenie sieci podstawowych (pikosieci). Ten typ systemu został nazwany siecią rozproszoną (*ang. scatternet*). Taki sposób organizacji systemu pozwala zwiększać liczbę wspólnie pracujących urządzeń. W ramach jednej sieci rozproszonej może współistnieć do dziesięciu sieci klasy "pikonet".

W zależności od sposobu organizacji wyróżnia się sieci z jednym urządzeniem będącym nadrzędnym (M) w jednej pikosieci, a podrzędnym w drugiej pikosieci. Przedstawiono to na

[14] *Razem w pikosieci osiem urządzeń aktywnych*

rysunku 4.1 b. W konfiguracji sieci rozproszonej jedno z urządzeń może zatem pełnić podwójną rolę - tzn. występuje zarówno w roli urządzenia podrzędnego jak i nadrzędnego.

Inną odmianę sieci rozproszonej jest system przedstawiony na rysunku 4.1 c. W tym przypadku wybrane urządzenia będą należeć do więcej niż jednej pikosieci.

Z przedstawionych konfiguracji i stosowanej hierarchii wynika, że dane urządzenie:

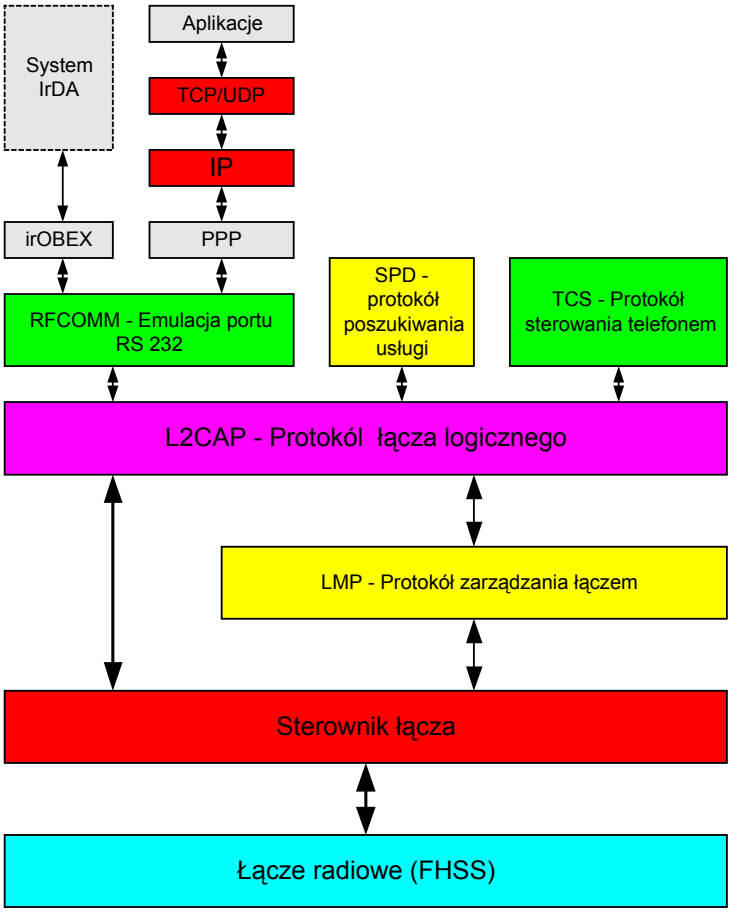
- może być podrzędnym w jednej piko sieci, a nadrzędnym w innej;
- może być urządzeniem podrzędnym w kilku pikosieciach;
- nie może być urządzeniem nadrzędnym w dwóch pikosieciach[15].

4.4 Architektura systemu Bluetooth

Architektura system Bluetooth przedstawiany jest zazwyczaj w postaci modelu warstwowego, w którym wyróżnia się:

- warstwę fizyczną - specyfikacja łącza radiowego (*ang. Radio Specification*);
- warstwę łącza danych - sterownik łącza (*ang. Baseband Specification*) wraz z protokołami zarządzania łączem - LMP (*ang. Link Management Protocol*) oraz łącza logicznego - L2CAP (*ang. Logical Link Control and Application Layer Protocol*);
- warstwy wyższe - protokoły wysokopoziomowe.

Architekturę systemu ilustruje rysunek 4.2.



Rys. 4.2. Architektura systemu Bluetooth

[15] *ponieważ dwie piko sieci nie mogą wykorzystywać tej samej sekwencji skoków częstotliwościowych.*

Najniższa warstwa radiowa definiuje wymagania wobec urządzeń nadawczych i odbiorczych. W ramach tej warstwy zdefiniowano trzy klasy urządzeń, których podstawowe dane zostały przedstawione wcześniej.

Warstwa sterownika łącza jest odpowiedzialna za logikę połączeń. W jej ramach wyróżnia się dwa protokoły:

- protokołami zarządzania łączem - LMP (*ang. Link Management Protocol*);
- protokół łącza logicznego - L2CAP (*ang. Logical Link Control and Application Layer Protocol*).

W ramach tej warstwy określa się pojęcie kanału transmisyjnego, jako pseudolosowej sekwencji skoków po (maksymalnie) 79 częstotliwościach. Sekwencja jest określana na podstawie adresu stacji nadrzędnej. Podstawowy kanał jest podzielony czasowo na szczelny po 625 μs, zaś stacje nadrzędne mogą nadawać tylko w szczelinach o numerach parzystych (urządzenia podrzędne w nieparzystych). W ten sposób uzyskiwana jest dwukierunkowość łącza (*ang. Time Division Duplex*). Transmisja ramek rozpoczyna się zawsze na początku szczeliny czasowej i może trwać, co najwyżej przez okres pięciu szczelin. Przeskoki częstotliwości są tak organizowane, aby cała ramka była nadana na jednej częstotliwości. Warstwa definiuje typy przesyłanych ramek, zapewnia ochronę przed błędami, szyfrowanie przesyłanych danych oraz synchronizację.

Następną podwarstwę tworzy protokół LMP (*ang. Link Manager Protocol*), który jest odpowiedzialny za zarządzanie łączem i jego konfiguracją oraz zmianą innych parametrów takich jak np. zmiany klucza szyfrującego w czasie trwania połączenia, modyfikacja ról urządzeń (nadrzędny/podrzędny). Za pomocą tego protokołu przesyłane są informacje umieszczane w ramce mieszczącej się w jednej szczelinie czasowej.

Przedstawione i opisane do tej pory warstwy zasadniczo muszą być umiejscowione w urządzeniu, zatem należą do tzw. części sprzętowej.

Następną podwarstwę tworzy protokół łącza logicznego - L2CAP (*ang. Logical Link Control and Application Layer Protocol*). Jest to w zasadzie pierwszy protokół implementowany programowo, a stosowany w łączach asynchronicznych - ACL. Podstawową funkcją tego mechanizmu jest multipleksacja danych pochodzących z warstwy wyższej. Innym zadaniem jest dopasowanie wielkości przesyłanych pakietów do rozmiaru ramek generowanych przez sterownik łącza[16]. L2CAP dba także o zachowanie parametrów QoS wynikających ze specyfikacji realizowanej usługi. Należy również dodać, że łącza synchroniczne (SCO), nie potrzebują adaptacji, stąd nie wymagają specjalizowanego protokołu.

W ramach warstwy wyższej można wyróżniać przykładowo następujące protokoły, które wykorzystywane są w konkretnych aplikacjach. Są to:

- protokół emulacji łącza szeregowego RFCOMM (emuluje działanie dziewięciu wyprowadzeń złącza RS 232);
- protokół poszukiwania (detekcji) usługi SDP - protokół nie warunkuje możliwości dostępu, a jedynie informuje urządzenia o dostępności określonych usług;
- protokół sterowania telefonem TSC (*ang. Telephony Control Specification*).

4.5 Transmisja głosu i danych

Protokół Bluetooth umożliwia przesyłanie sygnałów wymagających transmisji synchronicznych, takich jak sygnał mowy, a także sygnałów, które mogą być przesyłane asynchronicznie, czyli dane. Zdefiniowane są dwa typy łącz:

- Łącza synchroniczne (*SCO - Synchronous Connection Oriented*)
- Łącza asynchroniczne (*ACL- Asynchronous Connection-Less*).

[16] *W tym przypadku wypełniana jest funkcja podobna do warstwy AAL w ATM*

Każdy z wymienionych typów łącza wykorzystuje własne rodzaje pakietów, które zapewniają albo większe prędkości transmisji przy mniejszej odporności na zakłócenia, albo większą odporność na zakłócenia przy mniejszej prędkości transmisji. Najszybszą transmisję umożliwiają pakiety typu DH5, które zajmują pięć szczelin czasowych. Pozwalają one na uzyskanie maksymalnej przepustowości w jednym kierunku równej 723,2 kbit/s. Pakiety zwrotne o długości jednej szczeliny zapewniają przepływność 57,6 kbit/s. Jeśli pakiety DH5 są przesyłane w obu kierunkach, uzyskana przepływność na poziomie aplikacji wynosi około 650 kbit/s. Łącza SCO zapewniają przepływność 64 kbit/s. W tym samym czasie w jednej pikosieci mogą istnieć trzy takie łącza.

4.6 Wykrywanie dostępnych urządzeń i usług

Ze względu na doraźny charakter tworzenia sieci urządzeń Bluetooth (tryb *ad hoc*), znaczącą rolę odgrywa proces wykrywania urządzeń znajdujących się w danej chwili w zasięgu oraz pobierania informacji o usługach, które oferują wykryte urządzenia. Operacje te są realizowane bez udziału użytkownika.

Proces wykrywania rozpoczyna urządzenie wysyłające specjalne pakiety opatrzone kodem GIAC (*ang. General Inquiry Access Code*), po dwa w pojedynczej szczelinie czasowej, które następnie nasłuchuje odpowiedzi w kolejnej szczelinie. Wykorzystywana jest przy tym specjalna szybka sekwencja skoków częstotliwościowych (dwa skoki w jednej szczelinie czasowej). Urządzenie oczekujące na wykrycie nasłuchuje pakietów z kodem GIAC, stosując przy tym znacznie wolniejszą sekwencję skoków częstotliwości. Po odebraniu pakietu z kodem GIAC wysyła ono w odpowiedzi pakiet FHS (*ang. Frequency Hop Synchronization*), dzięki któremu oba urządzenia mogą się zsynchronizować.

Aby odpowiedzi dwóch urządzeń, które odebrały jednocześnie pakiet urządzenia wykrywającego nie zakłóciły się, każde urządzenie po odebraniu pakietu wstrzymuje nadawanie, a następnie czeka przez pewną losową liczbę szczelin czasowych i ponownie rozpoczyna nasłuchiwanie; odpowiadając po ponownym odebraniu pakietu z tym samym kodem GIAC. Po nawiązaniu połączenia wykryte urządzenie przesyła do urządzenia wykrywającego informacje o udostępnianych usługach. Służy do tego specjalny protokół SDP (*ang. Service Discovery Protocol*). W wyniku takiego procesu urządzenie wykrywające gromadzi w swojej pamięci informacje o urządzeniach, które zostały wykryte i usługach, które one realizują. Wyboru urządzenia, z którym ma być nawiązane połączenie, może dokonać użytkownik albo odpowiednia procedura programowa – wybór zależy od wykorzystywanej aplikacji.

4.7 Wywoływanie i nawiązywanie połączenia

Mechanizm nawiązywania połączenia jest podobny do wykorzystywanego podczas wykrywania dostępnych urządzeń. W celu nawiązania połączenia urządzenie inicjujące pobiera odpowiedni rekord z własnej bazy danych dostępnych urządzeń i kieruje bezpośrednie żądanie do stacji, z którą chce nawiązać połączenie. Wywoływane urządzenie musi być w stanie oczekiwania na wywołanie i nasłuchiwać pakietów zawierających własny adres. Gdy urządzenie wywoływane odbierze taki pakiet, potwierdza możliwość nawiązania połączenia, przesyłając w odpowiedzi ramkę zawierającą ten sam adres. Ponieważ adresy mają charakter unikalny, nie ma niebezpieczeństwa, że na wywołanie odpowie kilka urządzeń. Stacja wywołująca po odebraniu potwierdzenia wysyła pakiet FHS. W oparciu o zawarte w nim informacje urządzenie wywołane wyznacza sekwencję skoków częstotliwościowych urządzenia wywołującego i zaczyna ją stosować. Następuje ostateczne nawiązanie połączenia. Urządzenie wywołujące staje się urządzeniem nadrzędnym, a urządzenie wywoływane urządzeniem podrzędnym. Po przełączeniu na nową sekwencję skoków częstotliwościowych urządzenie nadrzędne wysyła pakiet kontrolny, którego zadaniem jest sprawdzenie poprawności nawiązanego połączenia.

4.8 Tryby pracy z oszczędzaniem energii

W przypadku urządzeń przenośnych znaczącą rolę odgrywa minimalizacja zużywanej energii. Najprostszym rozwiązaniem jest wyłączanie urządzenia, gdy nie jest ono używane. Z drugiej jednak strony tworzenie łącza zajmuje określony czas, więc nawiązywanie połączenia od nowa za każdym razem, gdy trzeba przesłać dane, nie jest korzystne. Na przykład, gdy używany jest zestaw słuchawkowy współpracujący z telefonem komórkowym, ważne jest, aby w przypadku odbierania połączenie, transmisja mogła być rozpoczęta jak najszybciej. Jednocześnie ciągłe utrzymywanie w aktywności łącza między zestawem słuchawkowym a telefonem jest niepotrzebne, ponieważ jest ono wykorzystywane sporadyczne.

W specyfikacji Bluetooth problem energooszczędności rozwiązano wprowadzając trzy podstawowe tryby pracy:

- *Hold* - urządzenie jest nieaktywne przez pewien pojedynczy odcinek czasu,
- *Sniff* - urządzenie jest aktywne tylko w określonych szczelinach czasowych,
- *Park* - urządzenie jest aktywne tylko w określonych szczelinach czasowych i przestaje być aktywnym członkiem pikosieci.

Tryb *Hold* umożliwia zatrzymanie ruchu ACL na pewien czas; nie wpływa na ruch SCO. Może być on przydatny, gdy urządzenie chce sprawdzić, czy w jego zasięgu nie pojawiły się jakieś nowe stacje. Polecenie wstrzymania transmisji nie wymusza wyłączenia odbiornika. Wykorzystanie wolnych szczelin zależy wyłącznie od zadań danego urządzenia. Trybu *Hold* może zażądać zarówno urządzenie nadrzędne, jak i podrzędne.

Tryb *Sniff* umożliwia ograniczenie ruchu do okresowych szczelin nasłuchiwania. Ten tryb może być używany do ograniczania zużycia energii na łączach o małych prędkościach transmisji. Urządzenie nadrzędne i podrzędne negocjują pozycję pierwszej szczeliny nasłuchiwania i przedział czasowy między kolejnymi szczelinami nasłuchiwania.

Urządzenie pracujące w trybie *Park* oddaje swój adres członka pikosieci i przestaje być jej aktywnym składnikiem. W trakcie przebywania w trybie *Park* nie wolno transmitować i nie można bezpośrednio odbierać transmisji urządzenia nadrzędnego pikosieci. Stacja jest uruchamiana okresowo, aby mogła nasłuchiwać komunikatów uaktywniających w wyznaczonych szczelinach sygnalizacyjnych.

4.9 Profile zastosowań

Urządzenia Bluetooth pochodzące od różnych producentów powinny ze sobą poprawnie współpracować, stąd w dokumentacji standardu zdefiniowano kilka profili zastosowań, które wskazują sposób realizacji określonych implementacji protokołu. Profile te obejmują między innymi takie zastosowania, jak: zestaw słuchawkowy, telefonia bezprzewodowa, transmisja danych, bezprzewodowy dostęp do sieci Internet (*Dial-up Networking*), bezprzewodowy dostęp do sieci lokalnej itp. I tak na przykład profil telefonii bezprzewodowej definiuje wykorzystanie przenośnego telefonu wyposażonego w interfejs Bluetooth do nawiązywania połączeń ze stacjami bazowymi różnych typów. Telefon taki może się łączyć ze stacjami bazowymi telefonii stacjonarnej, ale także tworzyć łącze z telefonem komórkowym. Profil zestawu słuchawkowego definiuje sposób implementacji transmisji głosu między telefonem (stacjonarnym lub komórkowym) a zestawem słuchawkowym wyposażonym w słuchawkę i mikrofon.

4.10 Bezpieczeństwo (szyfrowanie i zabezpieczanie)

Choć zastosowanie transmisji z wykorzystaniem skoków częstotliwościowych samo w sobie utrudnia podsłuchanie sygnału, wymagania bezpieczeństwa stawiane transmisjom bezprzewodowym sprawiają, że konieczne jest wykorzystanie zaawansowanych mechanizmów szyfrowania. W specyfikacji Bluetooth do uwierzytelnienia urządzeń wykorzystywany jest algorytm o nazwie SAFER+. Jest on używany również do generowania klucza stanowiącego

podstawę działania mechanizmu szyfrującego, który po zainicjowaniu losowo wybraną liczbą wykorzystuje takie elementy, jak: adres i wartość zegara urządzenia nadrzędnego, klucz współużytkowany przez oba komunikujące się urządzenia itp.

Uwierzytelnienie, czyli sprawdzenie, że oba komunikujące się urządzenia korzystają z tego samego klucza, odbywa się w sposób, który nie wymaga jego przesłania, co redukuje możliwość jego przejęcia przez strony niepowołane. Sam proces uwierzytelniania odbywa się w sposób następujący: W pierwszej fazie oba urządzenia wymieniają między sobą losowo wygenerowaną liczbę, która posłuży im do zainicjowania mechanizmu szyfrowania. Następnie urządzenie inicjujące weryfikację wysyła do drugiego urządzenia inną liczbę przypadkową, która zostanie zaszyfrowana przy użyciu posiadanego klucza i odesłana do weryfikacji. Urządzenie weryfikujące szyfruje wygenerowaną wcześniej liczbę przy użyciu swojego klucza i porównuje z odebraną wartością. Jeśli obie otrzymane liczby są sobie równe, oznacza to, że do ich zakodowania użyty został ten sam klucz, a co za tym idzie oba urządzenia mogą utworzyć szyfrowane połączenia.

4.11 Sterowanie jakością usług (QoS)

Specyfikacja Bluetooth umożliwia jednoczesne komunikowanie się wielu różnych urządzeń za pośrednictwem wielu rozlicznych protokołów. Wiąże się z tym konieczność obsługi połączeń różnego typu, dla których muszą być spełnione wymagania związane z wykorzystywanym łączem, a dotyczące przepływności, niezawodności, opóźnień występujących podczas transmisji itd. W specyfikacji Bluetooth zostały omówione metody konfigurowania jakości usługi (QoS), które umożliwiają dostosowywanie właściwości łącza do potrzeb danej aplikacji czy protokołu.

Negocjowanie parametrów łącza odbywa się zwykle przy pierwszym jego tworzeniu. Z warstwy aplikacji do warstw niższych protokołu Bluetooth kierowane są żądania określające minimalne wymagane parametry, które stają się przedmiotem negocjacji pomiędzy łączącymi się urządzeniami. Jeśli żądane parametry zostaną zaakceptowane, urządzenie wywoływane wysyła potwierdzenie i może nastąpić ostateczne nawiązanie połączenia.

Jeśli utworzenie łącza o zadanych parametrach nie jest możliwe, w danej aplikacji musi zostać określone, czy ma być negocjowane utworzenie łącza o gorszych parametrach, czy też nastąpi rezygnacja z nawiązania połączenia. Innym rozwiązaniem może być wstrzymanie transmisji na łączach o mniejszym priorytecie, a przez to udostępnienie szerszego pasma dla bardziej wymagającego połączenia. Wynegocjowane parametry są nadzorowane przez cały czas trwania połączenia i mogą być renegocjowane, gdy nastąpi pogorszenie jakości transmisji spowodowane nieoczekiwanymi zakłóceniami, albo gdy aplikacja zażąda zmiany parametrów.

Ustawienie parametrów łącza odbywa się poprzez dobór typu transmitowanych pakietów, które zapewniają jakość przesyłania danych z żądaną jakością i prędkością [7]. Zdefiniowane typy pakietów pozwalają na zwiększanie przepustowości łącza kosztem jego niezawodności. Można to osiągnąć wydłużając pakiet i zmniejszając nadmiarowe dane związanych z detekcją i korygowaniem błędów. I odwrotnie, chcąc zwiększyć niezawodność transmisji można zastosować pakiety, które są krótsze i zapewniają lepsze wykrywanie i korekcję błędów, co jednak wiąże się z obniżeniem przepustowości.

4.12 Podsumowanie

Standard Bluetooth jest uniwersalnym systemem umożliwiającym tworzenie bezprzewodowych połączeń między urządzeniami różnego typu, pochodzącymi od różnych producentów. Dzięki temu może on stanowić alternatywę dla połączeń kablowych, które w przypadku małych przenośnych urządzeń są niewygodne. Specyfikacja Bluetooth definiuje pełny system od poziomu łącza radiowego do warstwy zastosowań. Wykrywanie urządzeń dostępnych w zasięgu, tworzenie połączeń, nadzorowanie jakości połączenia i wiele innych funkcji jest realizowanych bez udziału użytkownika, co sprawia, że rozwiązanie to jest bardzo łatwe i wygodne w użyciu.

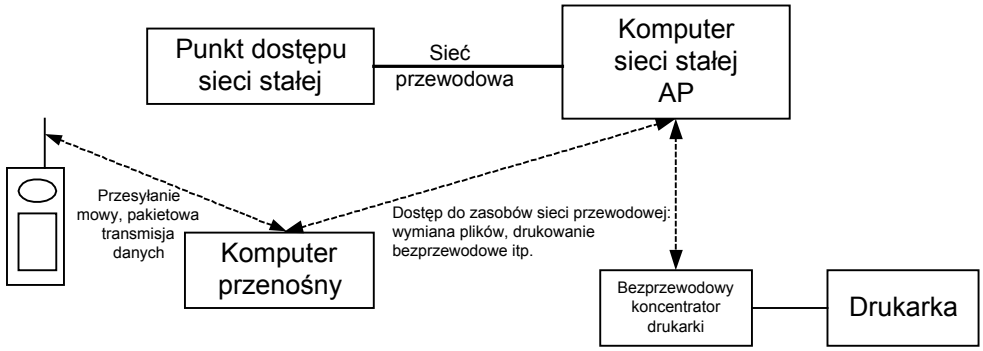
Bluetooth to jedna z najszybciej rozwijających się technologii ostatnich lat. Liczba firm biorących udział w pracach nad rozwojem projektu jest liczona w setkach. Działanie w powszechnie dostępnym paśmie ISM powoduje, że urządzenia Bluetooth mogą działać na całym świecie bez konieczności rezerwowania specjalnych zasobów. Ponieważ standard Bluetooth może działać jako protokół bazowy dla już istniejących protokołów, takich jak WAP, irOBEX (wymiany z systemem IrDA), czy też TCS, można go łatwo zaadaptować do pracy z już istniejącymi urządzeniami.

5 System IrDA

System IrDA (*ang. Infrared Data Assotiation*) jest firmowym systemem bezprzewodowej transmisji danych cyfrowych z wykorzystaniem podczerwieni. Został opracowany przez grupę skupiającą kilkudziesięciu producentów sprzętu komputerowego i przeznaczony jest głównie do tworzenia sieci doraźnych (tymczasowych), w których znajdują się komputery przenośne. W systemie tym zakłada się realizację następujących typów usług:

- Przesyłanie plików miedzy komputerami (podstawowa);
- Drukowanie (podstawowa);
- Dostęp do zasobów sieci przewodowej (dodatkowa);
- Transmisja danych i mowy miedzy komputerem a terminalem komórkowym (dodatkowa);
- Sterowanie urządzeniami telekomunikacyjnymi (dodatkowa).

Wymienione typy usług są dostępne bez konieczności dokonywania jakichkolwiek fizycznych połączeń sprzętu komputerowego. Ideę tego typu rozwiązania przedstawiono na rysunku 5.1.



Rys.5.1. Przykład obszaru zastosowań standardu IrDA

5.1 Architektura systemu

System bezprzewodowej transmisji danych cyfrowych z wykorzystaniem podczerwieni IrDA obejmuje trzy rodzaje elementów. Są to elementy występujące obowiązkowe, elementy opcjonalne oraz elementy multimedialne.

Do elementów obowiązkowych należą:

1. Schemat warstwy fizycznej - IrSIR
2. Protokół dostępu do łącza - IrLAP
3. Protokół zarządzania łączem - IrLMP

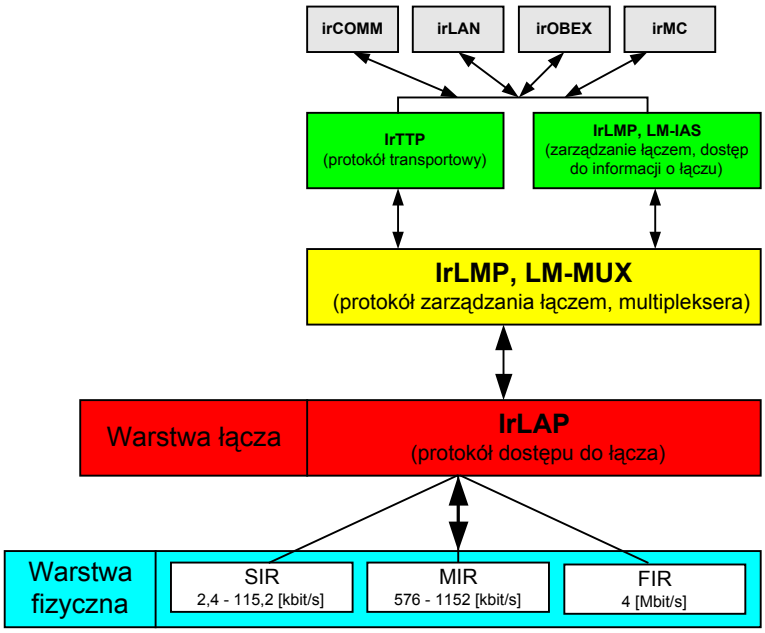
Do elementów opcjonalnych (nieobowiązkowych) należą:

1. Protokół transportowy - IrTTP
2. Zasady emulacji standardowych łączy z wykorzystaniem portów typu RS-232 i Centronics przy stosowaniu protokołów zgodnych ze standardem - IrCOMM
3. Rozszerzenie technologii *Plug and Play* - IrMP
4. Zasady współpracy z sieciami lokalnymi IrLAN
5. Zasady wymiany obiektów miedzy stacjami.

Do elementów multimedialnych należą:

1. Zasady przesyłania i reprezentacji obrazów cyfrowych - IrTran-P
2. Zasady współpracy ze sprzętem telekomunikacyjnym takimi jak np. terminale komórkowe - IrMC

Architekturę standardu IrDA zilustrowano w postaci warstwowej na rysunku 5.2.



Rys. 5.2. Architektura standardu IrDA

5.2 Warstwa fizyczna

Na poziomie warstwy fizycznej IrSIR *(ang. Serial Infrared)* zdefiniowane są następujące własności urządzeń:

- Prędkość transmisji od 2,4 kbit/s do 4 Mbit/s z zamiarem rozszerzenia do 16 Mbit/s;
- Rodzaj transmisji - asynchroniczna półdupleksowa;
- Komunikacja dwu- lub wielo punktowa;
- Odległość od stacji od 0,1 do 8 m[17];
- Kąt widzenia, co najmniej +/- 15^{o}; stacje mogą wykrywać transmisję przy różnych prędkościach, natomiast kolizje nie są wykrywane;
- Długość fali 850 do 900 nm.

W zakresie prędkości transmisji od 2,4 kbit/s do 4 Mbit/s wyróżnia się trzy zakresy:

- SIR - (*ang. Serial Infrared*) od 2,4 do 115,2 kbit/s;
- MIR - (*ang. Medium Infrared*) od 576 do 1152 kbit/s;
- FIR - (*ang. Fast Infrared*) - 4 Mbit/s.

Prędkości osiągane w zakresie SIR stanowią standardowy szereg wartości występujący w łączach szeregowych i wynoszą: 2,4; 9,6; 19,2; 38,4; 57,6 i 115,2 [kbit/s]. Przy zastosowaniu tych prędkości urządzenia zgodne ze standardem IrDA mogą współpracować bezpośrednio z typowymi układami transmisji szeregowej, np. UART (*ang. Universal Asynchronous Receiver - Transmitter*) czy interfejs standardu RS-232.

Sygnały przesyłane w łączu pracującym w zakresie podczerwieni kodowane są metodą RZI *(ang. Return to Zero Inverted)*.

Zakresy MIR i FIR wymagają zastosowania sterowników o możliwościach większych niż UART. Dla prędkości obowiązujących w zakresie MIR zasady kodowania są takie same jak dla zakresu SIR przy zmniejszeniu czasu trwania impulsu do 1/4 czasu trwania bitu.

[17] Zgodnie z obecnym standardem zasadnicza odległość od stacji wynosi 1 m, w planowanym systemie AIR (ang. *Area Infra Red*) proponuje się odległość 8 m.

Informowanie stacji pracującej z prędkościami transmisji z zakresu SIR o zajętości łącza przez stacje wykorzystujące większe szybkości jest realizowane poprzez okresowe wysyłanie sygnału SIP (ang. *Serial infrared Interaction Pulse*). Sygnał ten składa się z impulsu o czasie trwania 1,6 ms, po którym następuje 7,1 ms ciszy. Sygnał ten jest zazwyczaj nadawany bezpośrednio po wysłaniu całego pakietu.

Przy szybkościach transmisji 4 Mbit/s stosowana jest modulacja typu 4 - PPM *(ang. Pulse Position Modulation).*

5.3 Protokół dostępu do łącza

Protokół dostępu do łącza IrLAP (ang. *Link Access Procedure*) standardu IrDA jest oparty na protokole HDLC. Identyczny jest format ramki oraz wykorzystywana jest większość zdefiniowanych typów ramek. Różnice dotyczą jedynie sposobu wskazywania początku i końca ramki oraz sposobu uzyskania transparentności protokołu. Elementy te zależą od przyjętej prędkości transmisji warstwy fizycznej (tabela 5.1).

Tabela 5.1. Elementy protokołu IrLAP zależne od warstwy fizycznej

LP	Zakres	SIR	MIR	FIR
1.	Początek ramki	'C0h'	'7Eh'	Specjalne sekwencje bitów
2.	Koniec ramki	'C1h'	'7Eh'	Specjalne sekwencje bitów
3.	Przezroczystość protokołu	Wstawienie znaku sterującego '7Dh'	Szpikowanie zerami	Specjalne sekwencje bitów

5.4 Protokół zarządzania łączem

Protokół zarządzania łączem IrLMP (*ang. Link Management Protocol*) umożliwia:

- Zmianę liczby stacji w sieci w czasie jej pracy;
- Rozpoznanie usług oferowanych przez inne stacje;
- Pracę wielu niezależnych, współbieżnych aplikacji na jednym łączu.

Protokół zarządzania łączem składa się z dwóch części:

- Multipleksera - LM-MUX, zapewniającego dokonywanie wielu połączeń na jednym łączu;
- Systemu dostępu do informacji o łączu - LM-IAS, umożliwiającego stacjom uzyskanie informacji o stanie i możliwościach innych stacji.

5.5 Emulacja łącza i współpraca z sieciami lokalnymi

Protokół IrCOMM określa sposób emulacji standardowych łączy komunikacyjnych komputera z wykorzystaniem urządzeń standardu IrDA, Przyjęte rozwiązanie pozwala na zastąpienie połączeń przewodowych łączem optycznym w zakresie podczerwieni i zakłada całkowitą zgodność stosowanych urządzeń z oprogramowaniem używanym dla połączeń przewodowych. Standard przewiduje emulację czterech typów łączy:

- 3 przewodowych, prostych RS-232C (*ang. 3- wire raw*);
- 3 przewodowych RS-232C (*ang. 3- wire*);
- 9 przewodowych, prostych RS-232C (*ang. 9- wire*);
- Centronics.

Współpraca z sieciami LAN jest określana przez protokół IrLAN. Dzięki temu możliwy jest między innymi dostęp stacji do zasobów sieci lokalnej pomimo braku wyposażenia w karty sieciowe. Określone i dostępne są zasady współpracy standardu IrDA z popularnymi standardami takimi jak np. Ethernet, Token Ring itp. W zależności od rodzaju sieci LAN ulegają zmianie pewne parametry protokołu IrLAN miedzy innymi długość i format ramki. Obecnie przewidywane są trzy konfiguracje sieci:

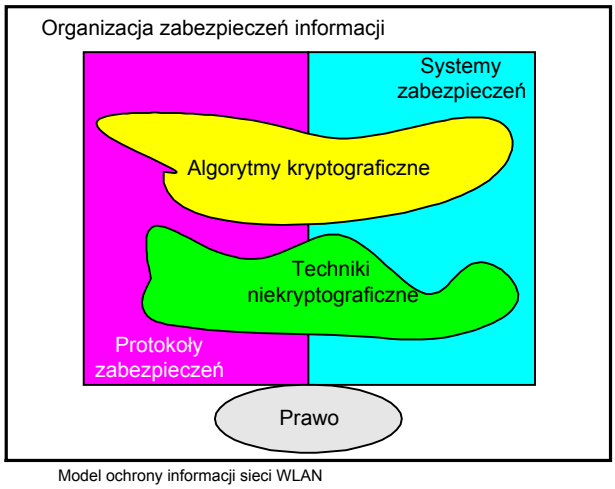
- Z punktem dostępu AP (*ang. access point mode*) w której każda stacja posiada indywidualny adres sieciowy;
- Partnerska (*ang. peer - to - peer mode*), w której stacje mobilne nie mają dostępu do zasobów sieci stałej - przewodowej;
- Z komputerem nadrzędnym (*ang. hostes mode*), w której stacje dzielą jeden wspólny adres sieciowy.

6 Ochrona informacji w sieciach WLAN

Współczesną ochronę informacji realizuje się w następujących obszarach. Są to:

- **Algorytmy kryptograficzne** - oparte na kryptografii szyfry, funkcje skrótu, algorytmy podpisu cyfrowego;
- **Techniki niekryptograficzne** - metody nie wywodzące się wprost z kryptografii - niekiedy bez wsparcia ze strony kryptografii nie stanowią w istocie żadnego zabezpieczenia; na przykład parametry zależne od czasu (ang. *Time Variant Parametrs*), techniki biometryczne (analiza kształtu dłoni, tęczówki, barwy głosu);
- **Protokoły zabezpieczeń** - realizują wybrane usługi bezpieczeństwa na przykład protokoły uwierzytelniania lub protokoły dzielenia sekretów;
- **Systemy zabezpieczeń** - rozbudowane aplikacje lub realizacje sprzętowe wybranych usług ochrony informacji - wykorzystują wybrane protokoły zabezpieczeń, np. systemy realizujące wirtualne sieci prywatne (protokoły uwierzytelniani, poufności i integralności) lub wykorzystują wyłącznie niekryptograficzne techniki zapewniania ochrony informacji, np. ściany ogniowe (firewall) i mechanizm filtrowania pakietów na podstawie list kontroli dostępu;
- **Organizacja zabezpieczeń** - zarządzanie zabezpieczeniami w systemach informacyjnych, przejawiające się oceną ryzyka projektu zabezpieczeń;
- **Prawo -** kwestie legislacyjne, które oddziałują na postać zabezpieczeń (w tym jakość).

W sposób graficzny model ochrony informacji przedstawiono na rys. 6.1.



Rys. 6.1. Model współczesnej ochrony informacji w sieciach WLAN

6.1 Ogólna charakterystyka algorytmów kryptograficznych

Na świecie rozwój algorytmów kryptograficznych charakteryzują dwa kierunki:

a) rozwój kryptoanalizy z wykorzystaniem technik obliczeń rozproszonych;
b) działania zapobiegające negatywnym skutkom kryptoanalizy.

Biorąc pod uwagę konstrukcję szyfrów, należy wspomnieć o istotnej zmianie w architekturze najnowszego systemu kryptograficznego - Rijndael, który jest następcą algorytmu DES (ang. *Data Encryption Standard*). Dotychczas w technikach kryptografii symetrycznej z zasady wykorzystywano tzw. schematy Feistela. Działanie najnowszego systemu kryptograficznego - Rijndael oparte jest na tych samych zasadach, jakie są wykorzystywane w kryptosysemach klucza publicznego, które wykorzystują zaawansowane narzędzia matematyczne.

Algorytm Rijndael jest szyfrem symetrycznym, w którym używa się kluczy o długości 128, 192 lub 256 bitów. Wspomniane długości klucza gwarantują bezpieczeństwo przez okres, co najmniej najbliższych paru dekad. Dla porównania: algorytm DES używa klucza o efektywnej długości 56 bitów, a algorytm 3DES - 112 bitów. Wraz z pojawieniem się nowego algorytmu symetrycznego, amerykański instytut NIST (*National Institute of Standards and Technology*) uaktualnił algorytm funkcji skrótu SHA (*Secure Hash Algorithm*), proponując nowe rozwiązania o symbolach SHA-256,SHA-384, SHA-512[18].

W dziedzinie podpisów cyfrowych nie wykorzystuje się nowych algorytmów i uważa się, że algorytm DSA (ang. *Digital Signature Algorithm*) o długości 160 bitów wciąż jest bezpieczny, choć przybywa powodów by uznać ten pogląd za nieuprawniony.

6.2 Techniki niekryptograficzne - ogólna charakterystyka

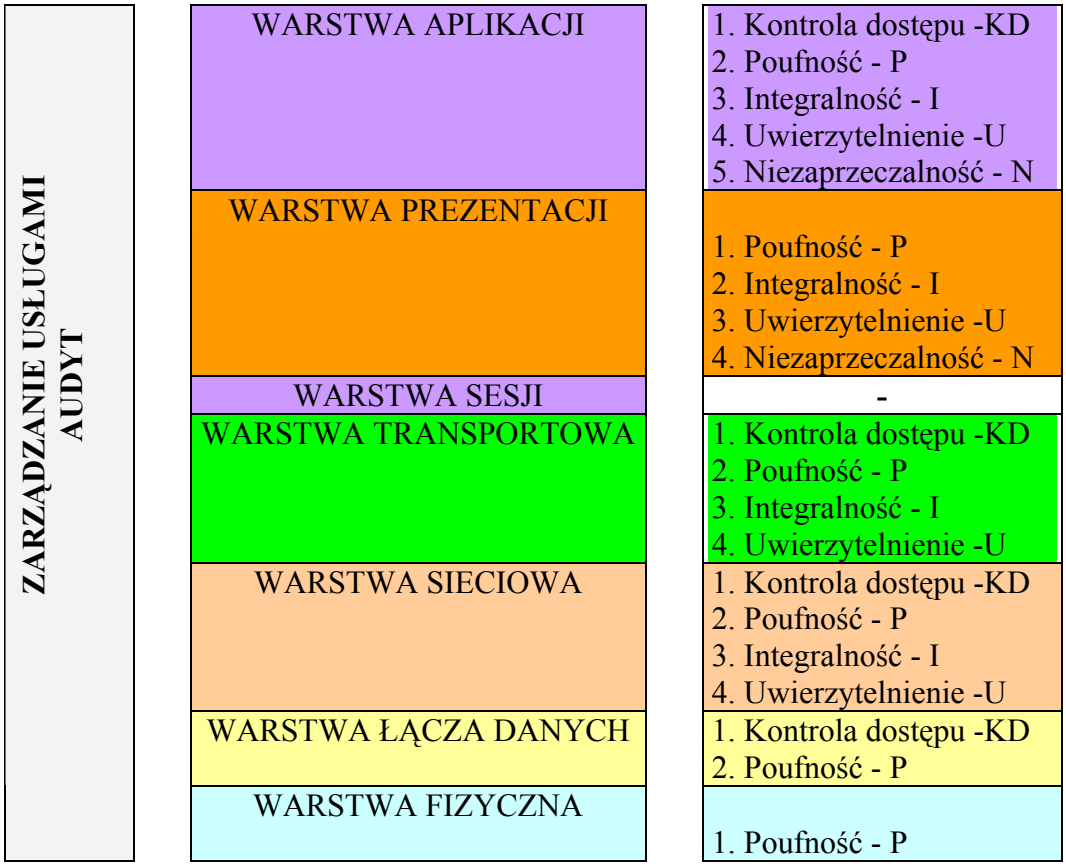
Wśród technik niekryptograficznych prym wiodą techniki biometryczne pozwalające na uwierzytelnianie osób, gdzie źródłem niezbędnych informacji mogą być m.in. linie papilarne, kształt dłoni, wzór siatkówki lub tęczówki, kształt twarzy, cechy pisma ręcznego (w tym podpisu), cech głosu. Biometryczne źródło uwierzytelnienia ma od kilkudziesięciu do kilkuset cech, które są poddawane analizie. Np. system uwierzytelniający na podstawie kształtu dłoni opiera się na około 100 cechach charakterystycznych, takich jak szerokość i grubość dłoni czy długość i grubość palców.

W praktycznych zastosowaniach coraz częściej spotyka się rozwiązania hybrydowe. W tego typu rozwiązaniach poza wykorzystywaniem kilku źródeł uwierzytelniania brane także są dane związane z miejscem pobytu danej osoby, otrzymane z jego osobistego odbiornika systemu lokalizacji GPS (ang. *Global Positioning System*). Masowe wykorzystanie technik biometrycznych umożliwi lepszą interakcję użytkowników z systemami teleinformacyjnymi, a także może usunąć bariery związane z zapamiętywaniem przez nich wielu kodów PIN i haseł.

6.3 Główne cechy protokołów zabezpieczeń

Lokalizacja usług ochrony informacji jest możliwa na poziomie wszystkich warstwach sieci przedstawiono na rysunku 6.2. W sieciach przewodowych nie ma wyraźnego trendu w zakresie implementowania usług ochrony informacji wraz z protokołami komunikacyjnymi. W sieciach bezprzewodowych - w dwóch najniższych ich warstwach - jest implementowana usługa poufności danych (mechanizm szyfrowania). Stosowane są przeważnie szyfry symetryczne pseudostrumieniowe (np. RC4) o kluczu ok. 64 bitowym, które najczęściej są celowo osłabiane np. klucz 40 bitowy. Zapewniana na tym poziomie ochrona, w połączeniu z wykorzystywanymi metodami transmisji - techniki z widmem rozproszonym FHSS czy DSSS zabezpiecza raczej przed przypadkowym podsłuchem, nie chroni zaś przed zaawansowanym atakiem. Niektóre z najpopularniejszych protokołów bezpieczeństwa używanych w sieciach bezprzewodowych, np. WEP (ang. *Wired Equivalent Privacy*) został wprowadzony wraz ze standardem IEEE 802.11. Protokół ten w wersji pierwotnej był obarczony błędami w konstrukcji, tj. niedbałym doborem wartości inicjujących, czy użyciem cyklicznego kodu nadmiarowego typu CRC-32 do zapewnienia usługi integralności.

[18] *Wymienione w symbolach liczby są długościami skrótów generowanych przez te algorytmy*



Rys. 6.2. Potencjalne możliwość realizacji usług ochrony informacji w modelu OSI/ISO.

Oprócz poufności w sieciach WLAN jest także realizowane uwierzytelnienie poszczególnych stacji (np. terminali i punktów dostępowych), głównie za pomocą technik symetrycznych ze wspólnym tajnym kluczem, połączonych z mechanizmem wezwanie-odpowiedź. W systemach telefonii komórkowej (GSM) 2 generacji, oprócz poufności w kanale radiowym jest realizowane uwierzytelnienie abonenta w sieci i poufność jego lokalizacji. W systemach trzeciej generacji (UMTS), które odziedziczył architekturę zabezpieczeń po GSM, dokonano jednak wzmocnienia część mechanizmów oraz rozszerzono obszar ich działania.

W latach 70 kiedy powstawała sieci teleinformatyczne, projektanci stosu protokołów TCP/IP podobnie jak twórcy systemów operacyjnych klasy Unix, nie mieli motywacji do wdrażania zabezpieczeń. Trudno było wtedy zakładać, że ktoś będzie chciał niszczyć czy nieuczciwie pobierać informacje z sieci, gdyż sieć tworzono w celu dzielenia się wiedzą a systemy operacyjne funkcjonowały poprawnie. Obecnie tego typu podejście jest nie do przyjęcia. Zabezpieczenia stosu TCP/IP są aktualnie implementowane:

- w warstwie sieciowej - zastąpienie IPv4 przez IPv6 lub uzupełnienie IPv4 przez Ipsec;
- w warstwie transportowej - dodanie protokołu realizującego poufność, integralność i uwierzytelnienie, zwanego TLS (ang. *Transport Layer Security*). [19]

Do ujednoliconych mechanizmów bezpieczeństwa dla IPsec i IPv6 zalicza się:

- *Authentication Header* (AH) - nagłówek uwierzytelniający, zapewniający integralność i uwierzytelnienie;
- *IP Encapsulating Security Payload (*ESP) - bezpieczna koperta, zapewniająca poufność zależnie od użytego algorytmu oraz trybu, także integralność i uwierzytelnienie.

Natomiast uwierzytelniona dystrybucja klucza kryptograficznego jest realizowana za pomocą protokołu IKE - *Internet Key Exchange*.

[19] Wcześniejsze wersje tego protokołu były znane pod nazwą SSL (ang. Secure Sockets Layer).

Bezpieczeństwo realizowane za pomocą protokołu TLS ogranicza się do aplikacji wykorzystujących protokół TCP (m.in. HTTP, FTP, SMTP, POP3). Został on zaadaptowany jako warstwa zabezpieczeń dla środowiska WAP (ang. *Wireless Application Protocol*) jako WTLS (ang. *Wireless Transport Layer Security*). Na poziomie aplikacji dużą rolę odgrywają usługi gwarantowania prywatności. Prywatność jest najczęściej realizowana przez poufność i uwierzytelnienie (systemy bezpiecznej poczty elektronicznej PEM - ang. *Privacy Enhancement for Internet Electronic Mail* i PGP - *Pretty Good Privacy*). Niekiedy prywatność jest osiągana przez zapewnienie anonimowości. W tym celu przeważnie wdraża się systemy anonimowego surfowania po Internecie i systemy anonimowego przesyłania wiadomości.

6.4 Charakterystyka systemów zabezpieczeń

Dość powszechnie stosowanym i znanym sieciowym systemem ochrony informacji jest firewall (ściana przeciwogniowa). W najprostszej postaci system ten jest filtrem, odrzucającym pakiety nadchodzące z określonych lokalizacji, a także odrzucającym niepoprawne jednostki danych. Firewall realizuje usługę kontroli dostępu, a także na podstawie generowanych logów umożliwia audit funkcjonalny systemu. Rozwiązanie to, mimo że najczęściej spotykane w sieciach TCP/IP, jest dostępny także dla sieci transferowania danych zrealizowanych w innych technikach np. ATM. Oprócz warstwy sieciowej i transportowej ściany przeciwogniowe mogą działać na poziomie protokołów warstwy aplikacji, służąc wtedy jako system pośredniczący. Ściany przeciwogniowe są umieszczane na styku sieci lokalnej z siecią rozległą lub w newralgicznych miejscach sieci lokalnej.

Innym ważnym systemem zabezpieczeń jest system wykrywania włamań (ang. *Intrusion Detection System*) - por. [8]. Jest to system wykrywający zachowania niezgodne z przyjętą definicją poprawnego zachowania się lub ewidentne naruszenie bezpieczeństwa systemu.

Systemy zarządzania nadużyciami FMS (ang. *Fraud Managment System*) są przeznaczone dla operatorów telekomunikacyjnych i mają wiele wspólnych elementów z systemami wykrywania włamań. Celem stosowania tego typu systemów jest głównie ograniczenie nadużyć dokonywanych przez abonentów albo nieuczciwy personel. Systemy zarządzania nadużyciami mogą czerpać informacje o aktywności bezpośrednio z systemów sygnalizacyjnych, np. SS7. Implementacja takich systemów wymaga stosowania kosztownych monitorów sieciowych, jednak poprawne umiejscowienie ich przy węzłach związanych z usługami, z którymi wiążą się największe nadużycia (połączenia międzynarodowe, usługi *premium-rate*), zapewnia wysoką skuteczność.

Wykrywanie włamań oraz złośliwego oprogramowania komplikuje przesyłanie danych w formie zaszyfrowanej. Systemy wykrywające włamania, wirusy, konie trojańskie i robaki przeprowadzają analizę semantyczną, która bez odszyfrowania danych jest bezwartościowa. Z tego powodu zauważalnym trendem jest integracja kryptosystemów szyfrujących ze wspomnianymi systemami wykrywania włamań i złośliwego oprogramowania.

Większość współczesnych kryptosystemów, realizujących poufność przez szyfrowanie, implementuje kompresję danych. Procesu kompresji dokonuje się wyłącznie przed zaszyfrowaniem danych, gdyż kompresja zaszyfrowanego strumienia danych jest nieefektywna.

Często kryptograficzna ochrona informacji jest stosowana do rozwiązań dotyczących wirtualnych sieci prywatnych VPN (ang. *Virual Private Network*). W sieciach TCP/IP najczęściej jest do tego używany wspomniany już protokół IPsec. Dopiero uzupełnienie o IPsec znanych rozwiązań VPN, takich jak PPTP (ang. *Point-to-Point Tunnelling Protocol*), L2TP (ang. *Layer Two Tunnelling Protocol*) gwarantuje prywatność w rozumieniu ochrony informacji. Także w systemach MPLS - VPN poufność jest najczęściej uzyskiwana przez protokół IPsec.

6.5 Istotne cechy organizacji zabezpieczeń

W organizacji zabezpieczeń rozważa się dwa aspekty tj. zarządzanie bezpieczeństwem oraz bezpieczeństwo zarządzania. Zarządzanie bezpieczeństwem to zarządzanie usługami i mechanizmami ochrony informacji. Jest ono realizowane przez dostarczanie informacji zarządzania do usług i mechanizmów, jak i informacji zbieranej oraz przechowywanie o usługach i mechanizmach. Z punktu widzenia organizacyjnego jest to proces projektowania, implementacji, oceny i eksploatacji zabezpieczeń.

Bezpieczeństwo zarządzania w ujęciu zbliżonym do TMN jest realizacją polityki bezpieczeństwa w zakresie zarządzania konfiguracją, wydajnością, uszkodzeniami, rozliczeniami, jak i samym jej bezpieczeństwem. Bezpieczeństwo systemu zarządzania jest traktowane jako atrybut systemu, związany z implementacją mechanizmów zapewniających: poufność, integralność, dostępność, rozliczalność i niezawodność. Dany stan bezpieczeństwa systemu zarządzania osiąga się przez zarządzanie bezpieczeństwem.

W ciągu kilku ostatnich lat dość znana i popularna, stała się infrastruktura klucza publicznego PKI (ang. *Public Key Infrastructure).* Stanowi ona platformę, która umożliwia tworzenie usług wykorzystujących certyfikaty klucza publicznego. Certyfikaty te są zbiorami danych, które zawierają: informacje o właścicielu certyfikatu, materiał klucza publicznego, datę ważności certyfikatu - całość potwierdzoną podpisem urzędu wystawiającego certyfikat, tj. urzędu ds. certyfikacji. Certyfikaty mogą być wystawiane zarówno ludziom jak i maszynom, stąd też istnieje możliwość wzajemnego certyfikowania urzędów. W ten sposób powstaje między urzędami łańcuch zaufania, dzięki któremu certyfikat wydany przez jeden urząd może być zweryfikowany przez odtworzenie ścieżki certyfikacji do drugiego urzędu, którego certyfikat jest znany dla sprawdzającego podmiotu.

Podstawowy problem w infrastrukturze klucza publicznego to wiarygodność certyfikatu. Przy wystawianiu certyfikatu wyróżnia się urząd ds. rejestracji, który jest odpowiedzialny za uwierzytelnienie tożsamości wnioskującego. Infrastruktura klucza publicznego od strony technicznej jest zdefiniowana w zaleceniu ITU X. 509. Użytkownicy infrastruktury klucza publicznego mają zazwyczaj możliwość realizacji procesów, takich jak::

- generacja pary kluczy (prywatny i publiczny);
- poufna wymiana klucza (dystrybucja lub uzgodnienie klucza);
- generacja podpisu cyfrowego;
- weryfikacja podpisu cyfrowego.

Dotychczas większość rozwiązań wykorzystujących algorytmy klucza publicznego zaprojektowano tak, aby współpracowały z infrastrukturą klucza publicznego. Są to m.in. TLS/SSL, S/MIME (*ang. Secure/Multipurpose Internet Mail Extensions*), SET (*ang. Secure Electronic Transactions*), PEM (*ang. Privacy Enhancement for Internet Electronic Mail*). Nadzieje wiąże się z bezprzewodową infrastrukturą klucza publicznego, tzw. *Wireless PKI* (W-PKI), dzięki której będzie możliwość dostępu do usług opartych na certyfikatach z poziomu terminala bezprzewodowego.

6.6 Szyfrowanie zgodne ze standardem 802.11

Popularnym sposobem szyfrowania w bezprzewodowych sieciach LAN (zgodnym ze standardem 802.11) realizowanym w warstwie 2 modelu OSI/ISO jest wykorzystaniem najpopularniejszego protokołu bezpieczeństwa WEP - (ang. *Wired Equivalent Privacy*), który charakteryzuje się:

1. Stosowaniem szyfru pseudostrumieniowego - RC4, o długości 40 lub 128- bitów;
   - Klucze szyfrujące:
     - Dla 40 bitowego - 10 cyfr hex (klucz w formie np. "klasa54321")
     - Dla 128 bitowego - 26 cyfr hex

2. Do wad szyfrowania z wykorzystaniem protokołu bezpieczeństwa WEP należą:
    - Współdzielone, statyczne klucze;
    - Brak centralnego zarządzania kluczami;
    - Słabe zabezpieczenia przed atakami.
3. Możliwość "złamania" kluczy poprzez pasywne odbieranie pakietów. Złamanie klucza może nastąpić po odebraniu około 500 - 1000 MB danych. (szacuje się, że dla 40 bitowego - 10 cyfr hex klucza złamanie może nastąpić w ciągu kilku dni). Posiadane wady WEP znacząco ograniczają jej zastosowanie w zasadzie do sieci, w których wymagany jest niski poziom zabezpieczeń kryptograficznych.
4. Przykład sposobów eliminacji wad protokołu bezpieczeństwa WEP
    - Szyfrowanie z wykorzystaniem dynamicznego klucza DSL (ang. *Dynamic Security Link*);
    - Realizacja mechanizmów bezpieczeństwa na wyższych warstwach modelu OSI/ISO (np. tunelowanie, VPN z wykorzystaniem IPSec itp.);
    - Realizacja funkcji kontroli dostępu do sieci zgodnych ze standardem IEEE 802.1x
5. Cechy szyfrowania z wykorzystaniem dynamicznego klucza DSL:
    - 128 - bitowa technika z kluczem dynamicznym;
    - Klucz jest negocjowany dla każdej sesji i dla każdego użytkownika;
    - Automatyczna wymiana kluczy;
    - Dołączenie się do sieci stacji mobilnej (klient) jest związane z koniecznością podania nazwy użytkownika i hasła;
    - Stacje pełniące rolę punktu dostępu do sieci (AP) powinny posiadać własną, wewnętrzną bazę danych użytkowników (np. produkty 3Com AP600/800 posiadają bazę dla 1000 użytkowników);
    - Wymagane jest zastosowanie bezprzewodowych kart sieciowych wspierających DSL;
    - Jest to stosunkowo dobre rozwiązanie dla małych firm, które chcą zapewnić bezpieczeństwo danych bez ponoszenia dodatkowych kosztów.
6. Cechy realizacji funkcji kontroli dostępu do sieci zgodnych z IEEE 802.1x:
    - Pozwala na uwierzytelnianie użytkowników z wykorzystaniem nazwy użytkownika i hasła;
    - Zapewnia wymianę kluczy;
    - Uwierzytelnienie w oparciu o EAP-TLS oraz EAP-MD5;
    - jako klient IEEE 802.1x jest standardowo dostępny w systemie Windows XP - i zapewnia dwustronne uwierzytelnienie bazowane na certyfikatach (EAP-TLS) oraz dynamiczną wymianę kluczy;
    - Musi współpracować z systemem uwierzytelniania np. RADIUS
7. Cechy IEEE 802.11x z wykorzystaniem autoryzacji EAP-MD5
    - Klient serwera RADIUS powinien być wbudowany w AP;
    - Autoryzacja klientów jest realizowana przez serwer RADIUS z wykorzystaniem protokołu EAP-MD5;
    - Istnieje możliwość uruchomienia szyfrowania typu WEP z kluczem 40 i 128 bitowym
    - Statyczne klucze wprowadzane są w koncentratorze bezprzewodowym oraz w każdym komputerze klienta;
    - Jest to dość dobre rozwiązanie dla firm wymagających centralnego zarządzania użytkownikami i wymaganiami w zakresie podstawowego zabezpieczenia danych.

8. Cechy IEEE 802.11x z wykorzystaniem autoryzacji EAP-TLS
    - Klient IEEE 802.1x jest dostępny standardowo w zasadzie tylko w systemie Windows XP;
    - Każdy klient sieci bezprzewodowej posiada unikalny certyfikat wydany przez zewnętrzny organ certyfikacji;
    - Serwer TLS musi również posiadać własny certyfikat wydany przez zewnętrzny organ certyfikacji;
    - Dobre rozwiązanie dla dużych firm wyposażonych w systemy operacyjne Windows XP oraz system PKI z certyfikatami dla każdej stacji końcowej
9. Cechy IEEE 802.11x z wykorzystaniem autoryzacji EAP-TLS-MD5
    - Klient RADIUS jest wbudowany w koncentrator bezprzewodowy;
    - Uwierzytelnienie z wykorzystaniem klienta 802.1X;
    - Uwierzytelnienie bazujące na certyfikatach z wykorzystaniem uniwersalnego certyfikatu klienta;
    - wymiana kluczy dynamiczna powinna być wspierana przez AP;
    - Uwierzytelnienie poprzez sprawdzenie nazwy użytkownika i hasła po przeprowadzeniu certyfikacji;
    - Wsparcie klienta 802.1X na systemach operacyjnych Windows;
    - Wsparcie standardowego szyfrowania algorytmem RC4 z kluczem 40 i 128 bitowym;
    - Jest to dobre rozwiązanie centralnego uwierzytelniania i zarządzania dużą liczbą użytkowników
10. Cechy kontroli dostępu adresów kart sieciowych w podwarstwie MAC
    - Większość AP pozwala na realizację uwierzytelnienia w oparciu o adres MAC karty sieciowej klienta;
    - AP powinna posiadać lokalną bazę danych MAC;
    - Możliwość uwierzytelnienia w oparciu o zewnętrzny serwer RADIUS zawierający bazę adresów MAC;
    - Możliwość szyfrowania danych WEP z kluczami 40 i 128 bitowymi.
11. Bezpieczeństwo na wyższych warstwach modelu OSI/ISO może być realizowane przez aplikacje sieciowe realizowane tak jak w tradycyjnych sieciach Ethernet np. VPN, IPsec, logowanie, szyfrowanie aplikacji.

6.7 Synchronizacja

Wszystkie stacje wewnątrz danego BSS powinny być zsynchronizowane. Procedury synchronizacji są wykorzystywane przez funkcje zarządzania poborem mocy stacji, zarządzania warstwą fizyczną (FHSS) oraz ramkowania usług izochronicznych CFS. W każdej stacji procedurami synchronizacji zajmuje się funkcja TSF (ang. *Timing Synchronization Function*). W sieci stałej za synchronizację odpowiadają stacje realizujące funkcje punktów dostępu.

6.8 Uruchomienie szyfrowania WEP z kluczem 40 oraz 128 bitowym

6.8.1 Uruchomienie szyfrowania w środowisku Windows XP.

1. Uruchomienie szyfrowania między urządzeniem AP a kartą sieciową:
   - powinno być zrealizowane na obu elementach;
   - rozpocząć się od konfiguracji szyfrowania na karcie bezprzewodowej;
   - urządzenia AP powinny być wstępnie skonfigurowane.
2. Prawym przyciskiem myszy wybieramy ikonę bezprzewodowego połączenia sieciowego (w podobny sposób jak w przypadku podłączenia karty sieciowej do koncentratora bezprzewodowego bez szyfrowania) i wybieramy opcję ***"View available wireless networks"***
3. Pojawia się okno wraz z wykazem wszystkich dostępnych nazw sieci.
4. Nazwy sieci są rozgłaszane przez koncentratory bezprzewodowe[20]. Zaznaczenie sieci o nazwie " Kadry" powoduje przedstawienie informacji o tym, że sieć wymaga użycia klucza WEP.
5. W polu "***Network key***" istnieje możliwość wpisania klucza do szyfrowania.
6. W tym przypadku predefiniowany klucz w urządzeniu AP ma postać dziesięciu cyfr w postaci heksadecymalnej (0-9, A, B, C, D, E, F). Każda cyfra jest kodowana czterobitowym słowem (co dla dziesięciu cyfr daje 40 bitową długość klucza)
7. Zakładamy, że predefiniowany klucz dla sieci (taki sam jak wpisany w koncentratorze bezprzewodowym) ma postać: " 1234512345".
8. Po poprawnym wpisaniu klucza wybieramy i naciskamy klawisz "*Conect*" (widoczny w oknie *"Conect to Wireless Network"*). Po wykonaniu tej operacji nastąpi dołączenie do sieci z wykorzystaniem szyfrowania WEP 40 bitów.
9. System Windows XP zapisuje ustawienia i kolejne dołączenia do sieci odbywa się już bez konieczności ręcznego wpisywania klucza.
10. Transmisja danych jest szyfrowana ostatnio wpisanym kluczem szyfrowania.
11. Jeżeli chcemy wykorzystać klucz szyfrowania o długości 128 bitów postępujemy dokładnie tak samo jak w przypadku klucza 40 bitowego, tzn. w polu okna "***Network key***" wpisujemy klucz do szyfrowania o odpowiedniej długości 26 znaków np.: "5432112345 54321123 aabbccdd"

6.8.2 Uruchomienie szyfrowania w systemie 3Com

1. W pierwszym kroku należy dokonać przełączenia obsługi karty bezprzewodowej z aplikacji systemu operacyjnego Windows XP na aplikację 3Com.
2. Uruchamiamy aplikację "*WLAN Launcher*"
3. Wybieramy ikonę kłódki (pojawi się ekran tej aplikacji *"3Com WLAN Configuration Utility"*)
4. W zakładce Network/Security (okna *"3Com WLAN Configuration Utility"*) obszaru wybieramy opcję 40 lub 128 bitową długość klucza szyfrowania:
   - Opcja 40-bit - w polu *"WLAN Service area"*: wybieramy opcję; *"3Com szyfracja 40-bit"*;

[20] *Funkcję tę można wyłączyć w koncentratorze bezprzewodowym w trakcie konfiguracji urządzenia AP.*

- Opcja 128-bit - w polu *"Security seting"*: wybieramy opcję *"128-bit Shared Key"*;

5. W celu wpisania klucza przyciskamy klawisz *"Encription Key"*. Po pojawieniu się pola wpisujemy poprawną wartość klucza.

Uruchomienie szyfrowania z dynamicznym kluczem 128-bitowym z wykorzystaniem DSL[21]

1. Szyfrowanie z wykorzystaniem dynamicznego klucza o długości 128 bitów (DSL) nie jest obsługiwane przez system operacyjny Windows XP.
2. Wykorzystywany w DSL 128-bitowy dynamiczny klucz, jest generowany na podstawie dodatkowo podanej nazwy użytkownika i hasła.
3. Szyfrowanie DSL jest dostępne w wybranych kartach oraz koncentratorach bezprzewodowych AP
4. Np. w produktach 3Com DSL występuje w kartach 3Com Wireless PC Card XJACK, AccessPoint 6000 oraz AccessPoint 8000.
5. Dla zobrazowania sposobu uruchamiania wykorzystany zostanie wcześniej omawiane oprogramowanie firmowe "*WLAN Launcher*", które uruchamiamy.
6. Wybieramy ikonę "kłódka" i w nowym oknie, w zakładce Network/Security wybieramy opcję *WLAN Service Area*: *"3Com szyfracja 40-bit", Security Setting: "128 Dynamic Security Link"*.
7. Pojawia się zakładka *"3Com 11 Mbps Wireless LAN Login"* w której podajemy nazwę użytkownika i hasło.
8. Po zatwierdzeniu zostanie podjęta próba dołączenia się do sieci bezprzewodowej. W wypadku pozytywnej weryfikacji zostaniemy dołączeni do sieci. W przeciwnym wypadku pojawi się stosowny komunikat.

6.8.3 Uwierzytelnienie użytkowników w oparciu o adresy MAC

(na przykładzie 11 Mbps Wireless LAN Access Point 8000 firmy 3Com)

1. Uwierzytelnienie dostępu do sieci bezprzewodowej na podstawie adresu MAC karty bezprzewodowej może być zrealizowana po podłączeniu się do koncentratora bezprzewodowego za pomocą przeglądarki WWW do systemu zarządzania konfiguracją "*Configuration Management System Version 1.1*"
2. W menu wybieramy zakładkę "***Encription***"
3. W wybranej zakładce obszar "***Security Settings***" wybieramy opcję uwierzytelniania klientów na podstawie adresów MAC (w lokalnej bazie danych adresów MAC) to znaczy zaznaczamy "***Local MAC Address with Access Point Encription***".
4. Wybieramy "***MAC Address Access List***" lub klikamy w miejsce "***Click here to set upthe MAC Address Access List"***, który znajduje się poniżej wcześniej zaznaczanego pola "***Local MAC Address with Access Point Encription***".
5. Po otwarciu się nowego okna widnieje lista adresów MAC. Aby wprowadzić (dodać) nowe adresy MAC tych kart sieciowych, które mogą się dołączać do koncentratora bezprzewodowego klikamy na link ***"Add new addresses"***
6. Po pojawieniu się nowego okna wpisujemy w pola wymagane adresy.

[21] *ang. Dynamic Security Link*

7. Autoryzacja karty sieciowej w oparciu o adres MAC jest realizowana w czasie dołączania się stacji (klienta) do sieci bezprzewodowej. Ponawiając próbę autoryzacji musimy wybrać sieć bezprzewodową, do której chcemy się dołączyć.

7 Łączenie stacji za pomocą bezprzewodowych kart sieciowych

7.1 Tryb doraźny

Połączenie stacji wyposażonych w bezprzewodowe karty sieciowe w trybie doraźnym, czyli bez pośrednictwa stacji pełniącej rolę AP jest możliwe po ręcznym zdefiniowaniu połączenia w trybie "partnerskim" (*peer - to - peer*) na wszystkich tych stacjach, które mają pracować w sieci *ad-hoc*.

Definiowanie nowego połączenia:

1. Otworzyć okno *"Network Connection"*. Prawym przyciskiem myszy zaznaczyć ikonę bezprzewodowego połączenia sieciowego w polu *"System Tray"* i wybrać opcję *"View available wireless networks"*
2. Po pojawieniu się okna *Connect to Wireless Network* w oknie *"Available networks"* zostaną wykazane wszystkie dostępnymi sieci bezprzewodowe sieci.
3. W celu wybrania jedynie stacje pracujące w trybie ad-hoc wybieramy opcję *"Advanced..."*. Pojawia się okno *Wireless Network Connection X Properties*, natomiast w polu tego okna *"Available networks"* wykazane zostaną wszystkie sieci bezprzewodowe, które zostały wykryte przez kartę sieciową naszej stacji. Stacje pracujące w trybie ad-hoc oznaczane są symbolem karty sieciowej. W celu odświeżenia konfiguracji sieci bezprzewodowych należy zaznaczyć przycisk *"Refresh"*, który umiejscowiony jest po prawej stronie okna.
4. Jeżeli z wykazanych wszystkich sieci chcemy wybrać tylko identyfikatory stacji pracujących w trybie ad-hoc wybieramy (ponownie) opcję *"Advanced..."*.
5. Po pojawieniu się okna *"Advanced"* w jego polu *"Network to access"* wybieramy i zaznaczamy pole *"Computer-to-computer (ad-hoc) network only"* oraz zatwierdzamy przyciskiem *"Close"*.
6. Definiujemy identyfikator sieci bezprzewodowej, którym będą posługiwały się wszystkie komputery biorące udział w połączeni. W dolnej części okna należy odznaczyć pole *"This is a computer-to-computer (ad-hoc) network; wireless access points are not used"*. Po zatwierdzeniu przyciskiem *"OK"* .
7. Pojawia się aktualne okno *Wireless Network Connection X Properties*, natomiast w polu tego okna *"Prefered networks"* wykazana została lista identyfikatorów stacji pracujących w trybie "ad-hoc". Zostały stworzone warunki do realizacji pożądanej komunikacji.
8. Prawym przyciskiem myszy zaznaczyć ikonę bezprzewodowego połączenia sieciowego w polu *"System Tray"* i wybrać opcję *"View available wireness networks"* W polu wyszczególnione są wszystkie dostępne sieci bezprzewodowe. Możemy wybrać stację z którą chcemy się komunikować bez pomocy stacji AP i zatwierdzić przyciskiem *"Connect"* i czekamy na zrealizowanie komunikacji.
9. Jeżeli chcemy sprawdzić do jakiej sieci jesteśmy podłączenia (np. *Wireless Network Connection X (Per-to-Per*), jaka jest aktualnie dostępna przepływność (np. 2 Mbps) lub jaki jest poziom sygnału (np. *"Low"*) powinniśmy naprowadzić kursor na ikonę bezprzewodowego połączenia sieciowego.
10. Jeżeli w trakcie operacji na tym etapie wybierzemy sieć bezprzewodową funkcjonującą w oparciu o stację AP zostanie wyświetlony komunikat o popełnionym błędzie.

7.2 Tryb z pośrednictwem stacji punktu dostępu AP

Próbę dołączenia się do wybranego punktu dostępowego AP sieci należy rozpocząć od otwarcia okna *"Network Connection"*

1. Prawym przyciskiem myszy zaznaczyć ikonę bezprzewodowego połączenia sieciowego w polu *"System Tray"* i wybrać opcję *"Open network connections"*.
2. Prawym przyciskiem myszy ponownie zaznaczamy ikonę bezprzewodowego połączenia sieciowego i wybieramy opcję *"View available wireness networks"*.
3. Pojawia się okno *"Network connections"*. W górnej części tego okna znajduje się lista aktualnie dostępnych sieci bezprzewodowych. Dokonujemy wyboru sieci i zatwierdzamy wybór przyciskiem *"Connect"* i oczekujemy na zrealizowanie komunikacji.

7.3 Zmiana komunikacji pomiędzy grupami roboczymi

Pracując w bezprzewodowej sieci LAN mamy możliwość dokonania zmiany i przeniesienia się do innej grupy roboczej. W tym celu należy:

1. Prawym przyciskiem myszy zaznaczamy ikonę bezprzewodowego połączenia sieciowego, w polu *"System Tray"* wybieramy opcję *"View available wireness networks"*.
2. W górnej części tego okna znajduje się lista aktualnie dostępnych sieci bezprzewodowych. Dokonujemy wyboru sieci i zatwierdzamy wybór przyciskiem *"Connect"* i oczekujemy na zrealizowanie komunikacji.
3. Zmiana grupy roboczej jest możliwa po zmianie ustawienia parametru identyfikacji sieci *"AreaID"*.

8 Wykaz literatury

1. Bing B.; High - Speed Wireless ATM and LANs. Artech House 2000, London, Boston
2. Breyer R, Rileyi S.; Switched, Fast i Gigabit Ethernet. Helion 2000, Gliwice.
3. Deboral Russell and..;Computer Security Basics. O'Reilly&Associates, INC. 1992
4. ETSI; TR 101 378 v. 1.1.1. Broadband Radio Access Networks (BRAN); Common ETSI - ATM Forum reference model for Wireless ATM Access Systems (WACS)
5. ETSI; TR 101 031 v.2.2.1. Broadband Radio Access Networks (BRAN) HIPERLAN Type 2
6. Nowicki K. Woźniak J.; Sieci LAN, MAN i WAN - protokoły komunikacyjne Fundacja Postępu Telekomunikacji, Kraków 1998
7. Tabbane S.; Handbook of Mobile Radio Networks. Artech House 2000, London, Boston
8. Zieliński B.; Bezprzewodowe sieci komputerowe. HELION 2000, Gliwice
9. Zienkiewicz R.; Telefony komórkowe GSM i DCS. WKŁ, Warszawa 1999 r.