802.11. Sieci bezprzewodowe. Przewodnik encyklopedyczny

Autor: Matthew S. Gast
Tłumaczenie: Arkadiusz Romanek, Witold Zioło
ISBN: 83-7361-163-0
Tytuł oryginału: 802.11 Wireless Networks: The Definitive Guide
Format: B5, stron: 476

Sieci bezprzewodowe dają poczucie wolności. Ale za tym poczuciem stoi złożony protokół i pojawiające się problemy, gdy wymiana danych nie jest ograniczona kablami. Jaką przyjąć strukturę sieci, by użytkownicy mogli skutecznie się w niej poruszać? Jak rozszerzyć zakres sieci radiowej, by można było z niej korzystać tam, gdzie zajdzie potrzeba? Jakie zagadnienia bezpieczeństwa wiążą się z sieciami bezprzewodowymi? Jak dostroić sieć, by pracowała wydajnie? Jak zapewnić wystarczającą początkową pojemność sieci i jak rozwiązywać problemy pojawiające się w miarę, gdy w sieci zaczyna pracować coraz to więcej użytkowników?

Książka „802.11. Sieci bezprzewodowe. Przewodnik encyklopedyczny" odpowiada na te i na wiele innych pytań. Przeznaczona jest dla administratorów odpowiedzialnych za instalację i funkcjonowanie sieci bezprzewodowej. W książce omówiono działanie protokołów 802.11 ze wskazaniem na dostępne możliwości i rozwiązywanie pojawiających się problemów. Zawiera ona także wyczerpujące omówienie zagadnień bezpieczeństwa sieci bezprzewodowych, łącznie z problemami protokołu WEP oraz omówieniem standardu bezpieczeństwa 802.1X. Monitorowanie sieci stało się obecnie potrzebą każdego administratora sieci, ale komercyjnych analizatorów sieci bezprzewodowych jest ciągle mało i są drogie, książka pokazuje, jak stworzyć analizator sieci bezprzewodowej wykorzystując do tego system Linux i oprogramowanie open source.

Poza omówieniem standardu 802.11b, książka „802.11. Sieci bezprzewodowe. Przewodnik encyklopedyczny" wybiega nieco w przyszłość w kierunku najnowszych technologii sieci bezprzewodowych, takich jak standardy 802.11a oraz 802.11g umożliwiające przesyłanie danych z prędkością 54 Mb/s. Omawia też inne prowadzone obecnie prace standaryzacyjne, mające na celu umożliwienie poruszania się między różnymi punktami dostępu, zapewnienie odpowiedniej jakości usług transmisji, zarządzanie sieciami oraz sterowanie mocą.

Książka „802.11. Sieci bezprzewodowe. Przewodnik encyklopedyczny" łączy niezbędną teorię z doświadczeniami i poradami praktycznymi potrzebnymi do uruchamiania sieci. Pokazuje też, jak skonfigurować bezprzewodowe karty sieciowe w systemach Linux, Windows oraz Mac OS X oraz jak konfigurować punkty dostępu.

Jeżeli administrujesz siecią bezprzewodową, ta książka jest dla Ciebie.

Wydawnictwo Helion
ul. Chopina 6
44-100 Gliwice
tel. (32)230-98-63
e-mail: helion@helion.pl

Spis treści

4

Ramki w sieciach 802.11 — więcej szczegółów

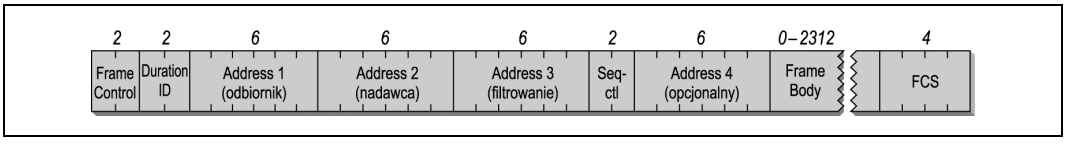
W rozdziale 3. przedstawiona została podstawowa struktura ramek oraz pola, które się na nią składają. Zabrakło w nim jednak szczegółów dotyczących różnych typów ramek. Ramkowanie w Ethernecie jest zagadnieniem bardzo prostym: dodaje się preambułę, trochę informacji adresowych, a na końcu dołącza się sumę kontrolną. Ramkowanie w sieciach 802.11 jest przedsięwzięciem zdecydowanie bardziej skomplikowanym, ponieważ nośnik bezprzewodowy pociąga za sobą obecność kilku funkcji zarządzających oraz odpowiadających im typów ramek, których nie spotyka się w sieciach przewodowych.

Istnieją trzy główne typy ramek. Ramki danych są „wołami roboczymi" specyfikacji 802.11, ciągnącymi dane od jednej stacji do drugiej. W zależności od sieci zaobserwować można kilka odmian ramek danych. Ramki kontrolne wykorzystuje się w połączeniu z ramkami danych w operacjach oczyszczania zasięgu, przejmowania kanału i utrzymania funkcji rozpoznania stanu nośnika oraz pozytywnego potwierdzania otrzymanych danych. Współpraca ta ma na celu zagwarantowanie niezawodnego przesyłu danych od stacji do stacji. Ramki zarządzające są odpowiedzialne za funkcje nadzorujące; służą do nawiązywania i zrywania kontaktu z sieciami bezprzewodowymi oraz zmiany skojarzeń z punktami dostępowymi.

Niniejszy rozdział został pomyślany jako punkt odniesienia. Niestety szczegóły dotyczące procesu ramkowania nie są tematem arcyciekawym, niezależnie od tego, jak bardzo autor będzie się starał pokolorować to zagadnienie. Czytelnik nie powinien czuć się zobligowany do natychmiastowego przeczytania tego rozdziału w całości. Równie dobrze może wrócić do niego, gdy wiedza na temat struktury ramek okaże się niezbędna. Precyzyjna znajomość relacji w procesie ramkowania, z rzadkimi wyjątkami, generalnie nie należy do kategorii: „o czym każdy administrator wiedzieć powinien". Rozdział ten jest równocześnie naszpikowany akronimami, warto będzie zatem konsultować się ze słownikiem pojęć z końca książki (dodatek C) w razie problemów z rozszyfrowaniem któregoś z nich.

Ramki danych

Ramki danych niosą w swojej treści dane protokołów wyższego poziomu. Na rysunku 4.1 zilustrowano ogólny schemat ramki danych. W niektórych typach ramek danych (w zależności od konkretnego typu ramki danych), niektóre z pól przedstawionych na rysunku mogą nie wystąpić.



Rysunek 4.1. Generalny schemat ramki danych

Ramki danych zostały podzielone na różne typy na podstawie sprawowanych przez nie funkcji. Jednym z takich podziałów jest rozróżnienie ramek danych wykorzystywanych do usług z rywalizacją o dostęp i bez takiej rywalizacji. Ramki, które pojawiają się tylko w okresie bez rywalizacji o dostęp, nie będą mogły nigdy zostać użyte w sieci IBSS. Kolejnym możliwym podziałem jest ten na ramki przenoszące dane i wykonujące funkcje zarządzające. Tabela 4.1 pokazuje, jak ramki mogą zostać podzielone na podstawie tych właśnie kategorii. Ramki wykorzystywane w usługach bez rywalizacji o dostęp zostały omówione szerzej w rozdziale 8.

Tabela 4.1. Kategorie ramek danych

Typ ramki	Usługa z rywalizacją o dostęp	Usługa bez rywalizacji o dostęp	Przenosi dane	Nie przenosi danych
Data	✓		✓	
Data+CF-Ack		✓	✓	
Data+CF-Poll		Tylko punkt dostępowy	✓	
Data+CF-Ack+CF-Poll		Tylko punkt dostępowy	✓	
Null	✓	✓		✓
CF-Ack		✓		✓
CF-Poll		Tylko punkt dostępowy		✓
CF-Ack+CF-Poll		Tylko punkt dostępowy		✓

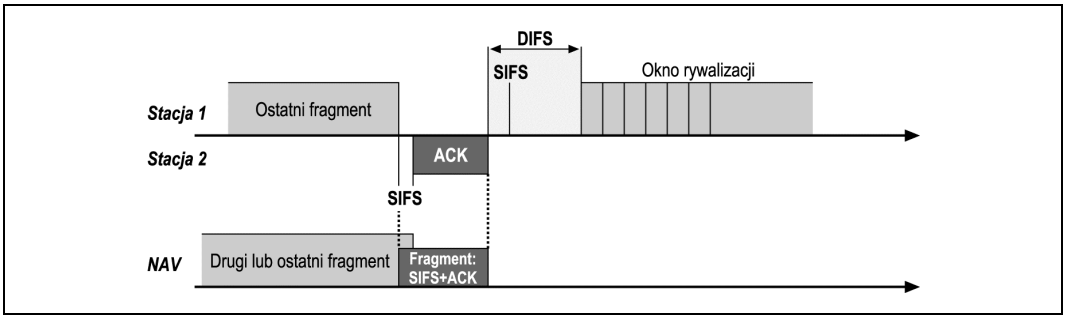
Frame Control

Wszystkie bity w polu Frame Control wykorzystuje się zgodnie z regułami opisanymi w rozdziale 3. Mogą one jednak wpłynąć na interpretację innych pól w nagłówku MAC. Do najbardziej znaczących elementów zależnych od wartości bitów ToDS i FromDS należą pola adresowe.

Duration

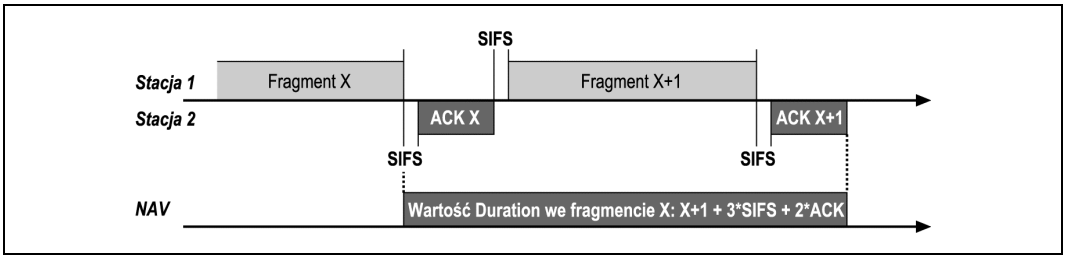
Pole Duration przenosi wartość wektora NAV — wektora alokacji sieci (*Network Allocation Vector*). Dostęp do nośnika jest ograniczony do czasu podanego w NAV. Ustawieniem pola Duration (okres trwania) w ramkach danych rządzą cztery reguły.

1. Wszystkie ramki przesyłane podczas okresu bez rywalizacji o dane ustawiają pole Duration na wartość 32 768. Dotyczy to dokładnie wszystkich ramek danych przesyłanych w tym czasie.
2. Ramki transmitowane do miejsc przeznaczenia typu broadcast i multicast (w polu Address 1. znajduje się bit adresu grupowego) otrzymują okres trwania równy 0. Ramki takie nie są częścią wymiany atomowej i nie są potwierdzane przez odbiorniki, tak więc nośnik jest dostępny zaraz po zakończeniu transmisji ramki danych typu broadcast i multicast i jest to dostęp oparty na rywalizacji. Wektor NAV służy do ochrony dostępu do nośnika transmisyjnego przez okres sekwencji wymiany ramek. Skoro po transmisji ramek typu broadcast i multicast nie ma potwierdzenia warstwy łącza danych, nie ma potrzeby blokowania dostępu do nośnika dla kolejnych ramek.
3. Jeśli bit More Fragments w polu Frame Control ma wartość 0, oznacza to, że w ramce nie ma już kolejnych fragmentów. Ostatni fragment musi zarezerwować nośnik tylko na transmisję swojego potwierdzenia, właśnie wtedy podjęta zostaje rywalizacja o dostęp. Pole Duration jest ustawione na odcinek czasu potrzebny na SIFS i potwierdzenie fragmentu. Rysunek 4.2 ilustruje ten proces. Pole Duration przedostatniego fragmentu blokuje dostęp do nośnika, żeby umożliwić transmisję ostatniego fragmentu.



Rysunek 4.2. Ustawienia pola Duration w ostatnim fragmencie

4. Jeśli bit More Fragments w polu Frame Control ma wartość 1, oznacza to, że do wysłania pozostały jeszcze jakieś fragmenty. Pole Duration ma ustawioną taką wartość, która odpowiada okresowi czasu potrzebnemu do transmisji dwóch potwierdzeń, trzech odstępów SIFS oraz kolejnego fragmentu. Zasadniczo każdy nieostatni fragment ustawia wektor alokacji sieci tak samo jak zrobiłby to RTS (patrz rysunek 4.3); z tego powodu o takim fragmencie mówi się *wirtualny RTS* (*virtual RTS*).



Rysunek 4.3. Ustawienia pola Duration we fragmencie nieostatnim

Adresowanie i bity DS

Liczba i funkcja pól adresowych zależy od tego, który z bitów systemu dystrybucyjnego jest ustawiony, a więc pośrednio wykorzystanie pól adresowych zależy od typu sieci. W tabeli 4.2 znajduje się podsumowanie zastosowania pól adresowych w ramkach danych.

Tabela 4.2. Zastosowanie pól adresowych w ramkach danych

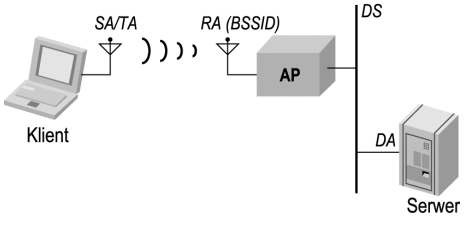
Funkcja	ToDS	FromDS	Address 1 (odbiornik)	Address 2 (nadajnik)	Address 3	Address 4
IBSS	0	0	DA	SA	BSSID	niewykorzystywane
Do punktu dostępowego (sieć stacjonarna)	1	0	BSSID	SA	DA	niewykorzystywane
Od punktu dostępowego (sieć stacjonarna)	0	1	DA	BSSID	SA	niewykorzystywane
WDS (most)	1	1	RA	TA	DA	SA

W polu Address 1 precyzuje się odbiorcę ramki. W wielu przypadkach adresem docelowym (DA — destination address) jest odbiornik (RA — receiver address), ale nie jest to regułą. Jeśli Address 1 jest ustawiony jako adres typu broadcast lub multicast, sprawdzany jest również BSSID. Stacje odpowiadają wtedy jedynie na ramki typu broadcast lub multicast pochodzące z tej samej grupy BSS. Address 2 to adres nadajnika (TA — transmitter address) i wykorzystywany jest podczas wysyłania potwierdzeń. Pole Address 3 służy punktom dostępowym i systemowi dystrybucyjnemu do filtrowania, jednak wykorzystanie tego pola zależy od typu zastosowanej sieci.

W przypadku sieci IBSS punkty dostępowe nie są jej częścią, a więc nie mamy tu do czynienia z systemem dystrybucyjnym. Źródłem (SA — source address) jest nadajnik, a miejscem docelowym — odbiornik. Wszystkie ramki niosą informację BSSID, żeby stacje mogły sprawdzać wiadomości typu broadcast i multicast; a jedynie stacje należące do tego samego BSS będą je przetwarzać. BSSID w sieci IBSS jest tworzony przez generator liczb losowych (*random-number generator — RNG*).

Standard 802.11 odróżnia źródło danych od nadajnika oraz analogicznie miejsce przeznaczenia danych od odbiornika. Nadajnik wysyła ramkę do nośnika bezprzewodowego, ale nie musi koniecznie być jej twórcą. Podobna różnica okazuje się być prawdziwa w przypadku adresów docelowych i odbiorników. Odbiornik może być pośrednim miejscem docelowym, ale ramki będą przetwarzane przez wyższe warstwy protokołu, dopiero gdy dotrą do swego celu.

Aby szerzej omówić to zagadnienie, przyjrzyjmy się wykorzystaniu pól adresowych w sieciach stacjonarnych. Rysunek 4.4 pokazuje prostą sieć, w której bezprzewodowy klient jest połączony z serwerem za pomocą sieci 802.11. Ramki wysyłane przez klienta do serwera posługują się polami adresowymi w sposób przedstawiony w drugiej linii tabeli 4.2.



Rysunek 4.4. Wykorzystanie pól adresowych w ramkach adresowanych do systemu dystrybucyjnego

BSSID

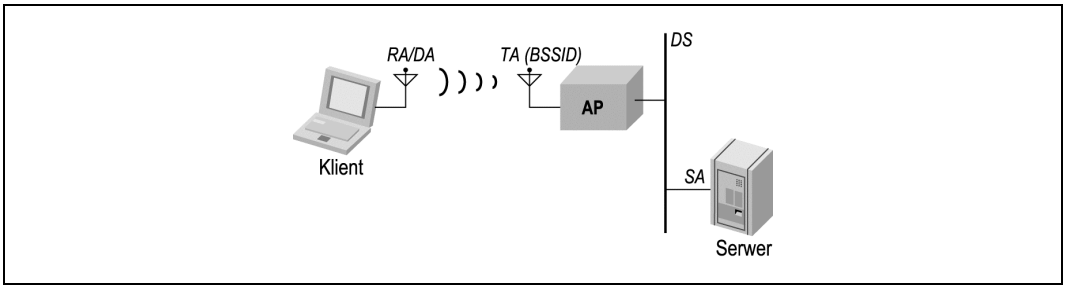
Każdy BSS posiada przypisany mu BSSID, tzn. 48-bitowy identyfikator binarny, który odróżnia każdy BSS od pozostałych BSS-ów w całej sieci. Główną zaletą identyfikatora BSSID jest funkcja filtrowania. Kilka niezależnych od siebie sieci bezprzewodowych może fizycznie się nakładać, a nie ma istotnego powodu, by jakaś sieć otrzymywała wiadomości typu broadcast warstwy łącza danych z sieci fizycznie nakładającej się.

BSSID w BSS-ach stacjonarnych to adres MAC bezprzewodowego interfejsu w punkcie dostępowym tworzącym dany BSS. IBSS, czyli BSS-y niezależne, muszą z kolei same tworzyć BSSID dla powstających sieci. Dla zwiększenia prawdopodobieństwa uzyskania niepowtarzalnego adresu generowanych jest 46 losowych bitów. Bit Universal/Local nowego BSSID otrzymuje wartość 1, co wskazuje na adres lokalny, niewykraczający poza granice BSS, a bit Individual/Group otrzymuje wartość 0. Uzyskanie identycznego BSSID dla dwóch osobnych sieci IBSS wymagałoby wygenerowania identycznych losowych 46 bitów.

Jeden adres BSSID jest zarezerwowany, a jest nim składający się z samych jedynek *broadcast BSSID* — BSSID rozgłoszeniowy. Ramki, które posługują się BSSID rozgłoszeniowym przechodzą przez wszelkie filtrowania w warstwie MAC. Transmisje BSSID broadcast są wykorzystywane, tylko w sytuacjach gdy stacje przenośne usiłują zlokalizować sieć, wysyłając ramkę Probe Request. Ramki te, by wykryć obecność sieci, nie mogą być filtrowane przez filtr BSSID. Jedynymi ramkami mogącymi posługiwać się BSSID rozgłoszeniowym są właśnie ramki typu Probe.

W przypadku ramek zaadresowanych do systemu dystrybucyjnego klient jest zarówno źródłem, jak i nadajnikiem. Odbiornikiem ramki bezprzewodowej jest punkt dostępowy, jednak jest on tylko pośrednim punktem docelowym. Kiedy ramka dociera do punktu dostępowego, jest przekazywana do systemu dystrybucyjnego, by mogła dotrzeć do serwera. Dlatego też punkt dostępowy jest odbiornikiem, a (ostatecznym) punktem docelowym jest serwer. W sieciach stacjonarnych punkty dostępowe tworzą stowarzyszone BSS-y za pomocą adresu swojego interfejsu bezprzewodowego i to właśnie dlatego adres odbiornika (Address 1) jest ustawiony na BSSID.

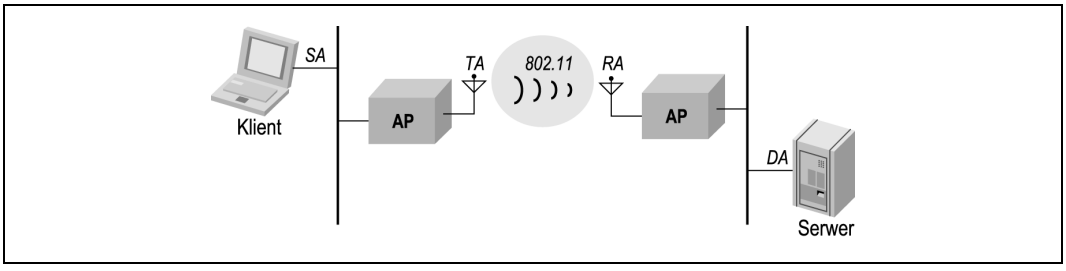
Kiedy serwer odpowiada klientowi, ramki są transmitowane do klienta przez punkt dostępowy, tak jak zostało to pokazane na rysunku 4.5. Scenariusz ten odpowiada zapisowi w trzeciej linii w tabeli 4.2.



Rysunek 4.5. Wykorzystanie pól adresowych w ramkach otrzymywanych od systemu dystrybucyjnego

Ramki są tworzone przez serwer, a więc adresem źródłowym ramek jest adres MAC serwera. Kiedy ramki są przekazywane przez punkt dostępowy, punkt ten podaje swój interfejs bezprzewodowy jako adres nadajnika. Tak jak w poprzednim przypadku, adres interfejsu punktu dostępowego jest również identyfikatorem BSSID. Ramki są w ostateczności wysyłane do klienta, który jest zarówno miejscem przeznaczenia, jak i odbiornikiem.

Czwarta linia w tabeli 4.2 ilustruje wykorzystanie pól adresowych w *bezprzewodowym systemie dystrybucyjnym* (*wireless distribution system — WDS*), czasami nazywanym *mostem bezprzewodowym* (*wireless bridge*). Na rysunku 4.6 dwie sieci przewodowe są połączone ze sobą punktami dostępowymi działającymi jako mosty bezprzewodowe. Ramki podróżujące od klienta do serwera muszą skorzystać z bezprzewodowego systemu dystrybucyjnego. Adresy źródłowy i docelowy ramki bezprzewodowej pozostają adresami klienta i serwera. Niemniej jednak ramki te wskazują również nadajnik i odbiornik ramki w nośniku bezprzewodowym. W przypadku ramek podróżujących od klienta do serwera nadajnikiem jest punkt dostępowy po stronie klienta, a odbiornikiem punkt dostępowy po stronie serwera. Oddzielenie źródła od nadajnika umożliwia punktowi dostępowemu po stronie serwera wysyłanie potwierdzeń wymaganych przez standard 802.11 do swojego odpowiednika po stronie klienta, całość połączenia nie koliduje z przewodową warstwą łącza danych.



Rysunek 4.6. Bezprzewodowy system dystrybucyjny

Wariacje na temat ramek danych

Specyfikacja 802.11 posługuje się kilkoma różnymi typami ramek danych. Odmiany te są zależne od tego, czy usługa jest oparta na rywalizacji o dostęp, czy też bez niej. Ramki w transmisji bez rywalizacji o dostęp w imię wydajności mogą realizować kilka funkcji. Ramki danych mogą więc transmitować dane, ale po zmianie ich podtypu; w okresie bez rywalizacji o dostęp będą wykorzystywane do potwierdzania innych ramek, co pozytywnie wpłynie na nadmiar odstępów międzyramkowych i oddzielnych potwierdzeń. Oto kilka powszechnie stosowanych podtypów ramek danych.

Podtyp *Data*

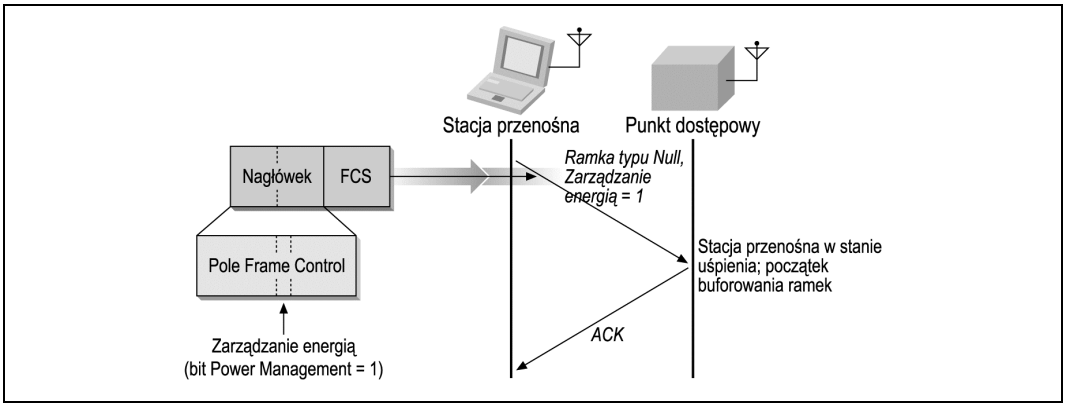
Ramki typu Data są transmitowane wyłącznie podczas okresów opartych na rywalizacji o dostęp. Są to zwykłe ramki przeznaczone wyłącznie do przenoszenia danych w treści ramki od jednej stacji do drugiej.

Podtyp *Null*

Ramki typu Null (zerowe)[1] są osobliwym tworem. Składają się z nagłówka MAC, po którym następuje pole końca ramki FCS. W tradycyjnym Ethernecie puste ramki byłyby uznane za dziwaczną przesadę; w sieciach bezprzewodowych wykorzystują je stacje przenośne do informowania punktów dostępowych o zmianach w trybie oszczędzania energii. Kiedy stacja przechodzi w tryb uśpienia, punkt dostępowy musi rozpocząć buforowanie ramek do niej adresowanych. Jeśli stacja przenośna nie ma danych do wysłania systemem dystrybucyjnym, może posłużyć się ramką typu Null z bitem Power Management ustawionym w polu Frame Control. Punkty dostępowe nigdy nie przechodzą w tryb oszczędzania energii oraz nie transmitują ramek typu Null. Sposób wykorzystania ramek typu Null przedstawiono na rysunku 4.7.

Istnieje również kilka innych typów ramek stosowanych w okresach bez rywalizacji o dostęp. Jednak usługa bez rywalizacji o dostęp nie jest powszechnie wykorzystywana. Analiza ramek nierywalizujących o dostęp (Data+CF-Ack, Data+CF-Poll, Data+CF-Ack +CF-Poll, CF-Ack, CF-Poll i CF-Ack+CF-Poll) znajduje się w rozdziale 8.

[1] Angielska nazwa typu ramki „Null" oznacza „zero". Aby odróżnić ramkę pustą (null frame) od ramki typu Null (Null frame), autor oryginału tej książki zwraca uwagę na potrzebę pisania tego drugiego wyrażenia wielką literą. Dotyczy to oczywiście języka angielskiego — *przyp. tłum.*



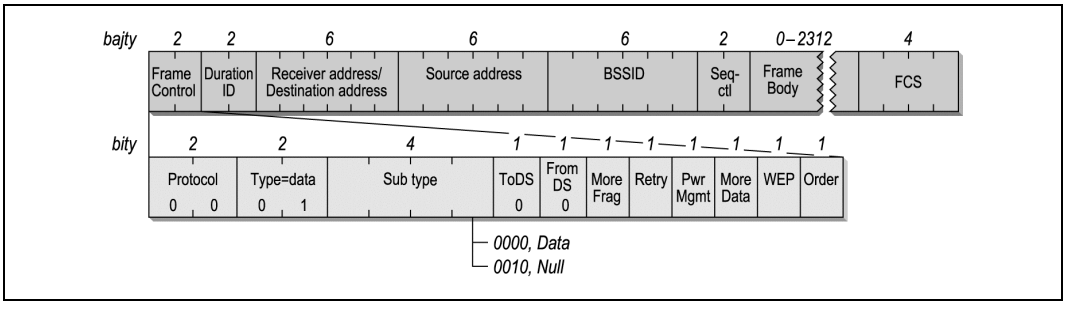
Rysunek 4.7. Ramka danych podtypu Null

Ramkowanie stosowane

Forma ramki danych zależeć może od typu sieci. Faktyczny podtyp ramki jest określany wyłącznie w polu podtypu (*subtype*) i nie wyraża się obecnością lub brakiem jakichkolwiek innych pól w ramce.

Ramki IBSS

W sieci IBSS stosuje się trzy pola adresowe, co pokazano na rysunku 4.8. Pierwszy adres identyfikuje odbiornik, który w przypadku IBSS jest również adresem docelowym. Drugi adres stanowi adres źródłowy. Po adresach źródłowym i docelowym ramki danych w sieci IBSS zostają opisane za pomocą BSSID. Kiedy bezprzewodowa warstwa MAC otrzymuje ramkę, sprawdza BSSID i przekazuje dalej tylko ramki w obecnym BSSID stacji do wyższych warstw protokołów.

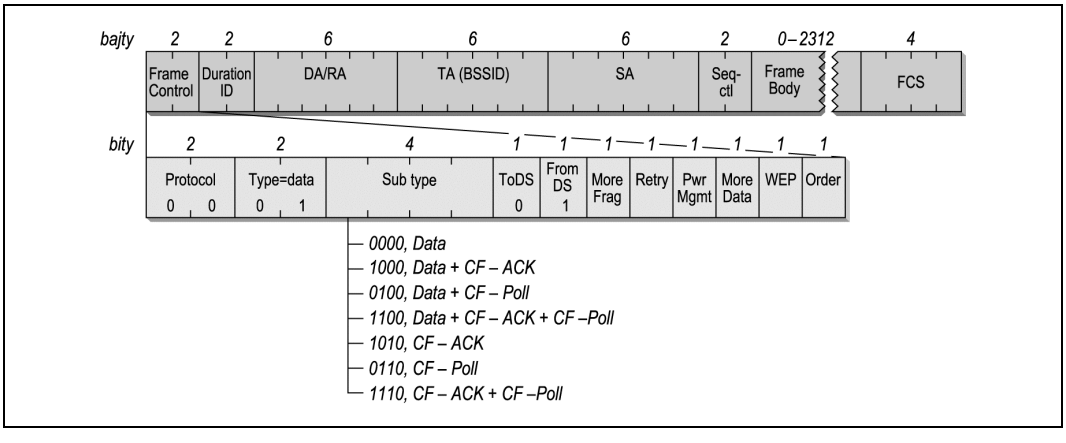


Rysunek 4.8. Ramki danych IBSS

Ramki danych IBSS występują w podtypach Data i Null; ten drugi służy do komunikowania o stanie zużycia energii.

Ramki wychodzące z punktu dostępowego (AP)

Rysunek 4.9 ilustruje format ramki wysyłanej z punktu dostępowego do stacji przenośnej. Tak jak we wszystkich ramkach danych, pierwsze pole adresowe oznacza w sieci bezprzewodowej odbiorcę ramki, będącego miejscem jej przeznaczenia. Drugi adres wskazuje na adres nadajnika. W sieciach stacjonarnych adres nadajnika jest adresem stacji w punkcie dostępowym, który jest również równy identyfikatorowi BSSID. Aż w końcu ramka podaje swój źródłowy adres MAC. Rozdział źródła od nadajnika danych jest konieczny, ponieważ warstwa MAC w standardzie 802.11 wysyła potwierdzenia do nadajnika ramki (punktu dostępowego), a warstwy wyższe wysyłają odpowiedzi na adres źródłowy ramki.

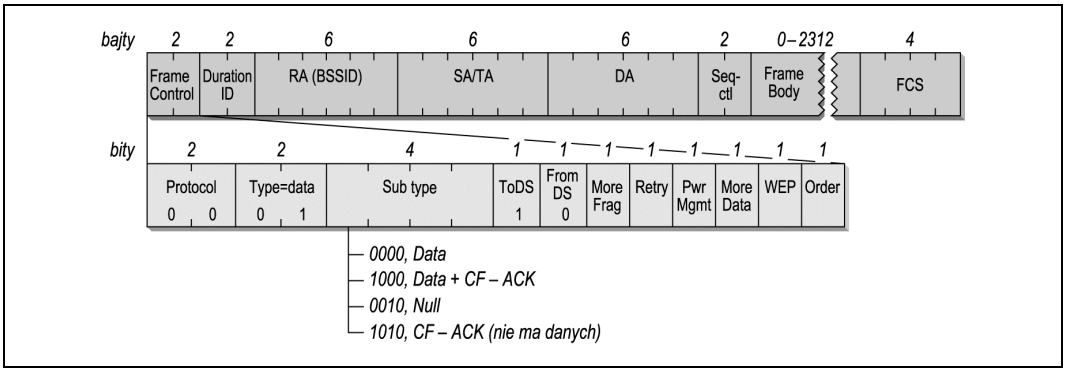


Rysunek 4.9. Ramki danych wychodzące z punktu dostępowego

W specyfikacji 802.11 nic nie zabrania punktom dostępowym transmitowania ramek typu Null, nie istnieje jednak żadna przyczyna, żeby je nadawać. Punktom dostępowym nie wolno posługiwać się procedurami oszczędzania energii i mogą one zatwierdzać ramki typu Null otrzymane od stacji bez wykorzystywania ramek typu Null do odpowiedzi. W praktyce punkty dostępowe wysyłają ramki typu Data w okresie dostępu do sieci opartego na rywalizacji, a ramki obsługujące funkcję CF-Poll — w okresach bez rywalizacji o dostęp.

Ramki adresowane do punktu dostępowego

Rysunek 4.10 ilustruje format ramki wysyłanej ze stacji przenośnej w sieci stacjonarnej do punktu dostępowego obsługującego ją w danej chwili. Adresem odbiornika jest BSSID. W sieciach stacjonarnych BSSID jest adresem MAC stacji sieciowej z punktu dostępowego. Ramki adresowane do punktu dostępowego otrzymują swój adres źródłowy (nadawcy) z sieciowego interfejsu w stacji bezprzewodowej. Punkty dostępowe nie wykonują operacji filtrowania, natomiast wykorzystują trzeci adres do przekazywania dalej danych do odpowiedniej lokalizacji w systemie dystrybucyjnym.

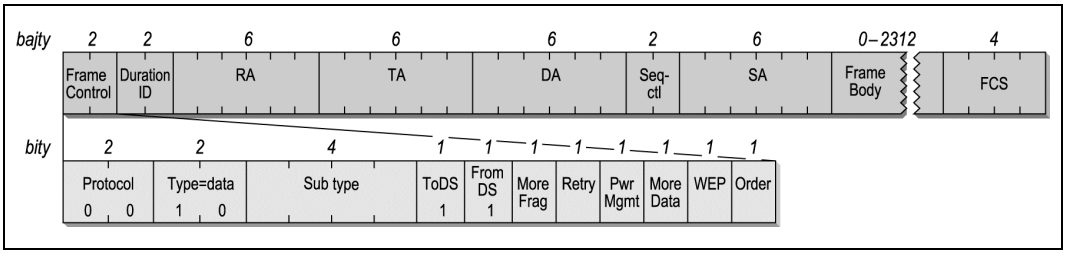


Rysunek 4.10. Ramki danych adresowane do punktu dostępowego

Ramki wychodzące z systemu dystrybucyjnego mają ustawiony bit ToDS, natomiast bit FromDS ma wartość 0. Stacje przenośne w sieci stacjonarnej nie mogą zostać koordynatorami punktu i dlatego nigdy nie wysyłają ramek, które są wyposażone w funkcje odpytywania w usłudze bez rywalizacji o dostęp (*Contention-Free Polling — CF-Poll*).

Ramki w bezprzewodowym systemie dystrybucyjnym

Kiedy punkty dostępowe zostają zastosowane w topologii wykorzystującej most bezprzewodowy (lub — mówiąc inaczej — bezprzewodowy system dystrybucyjny WDS), wykorzystywane są wszystkie cztery adresy, co pokazano na rysunku 4.11. Jak wszystkie inne ramki danych, ramki WDS stosują pierwszy adres dla odbiornika ramki, a drugi — dla nadajnika. Warstwa MAC posługuje się tymi dwoma adresami do potwierdzeń i ruchu kontrolnego, takiego jak ramki RTS, CTS i ACK. Dwa kolejne pola adresowe są potrzebne dla wskazania źródła i miejsca przeznaczenia ramki i odróżnienia ich od adresów wykorzystywanych w łączach bezprzewodowych.



Rysunek 4.11. Ramki WDS

W bezprzewodowym połączeniu mostkowym zazwyczaj nie umieszcza się żadnych stacji przenośnych i nie wykorzystuje się okresu bez rywalizacji o dostęp. Punkty dostępowe otrzymują zakaz wchodzenia w tryb oszczędzania energii, a więc bit zarządzania energią jest zawsze ustawiony na wartość 0.

Ramki wykorzystujące WEP

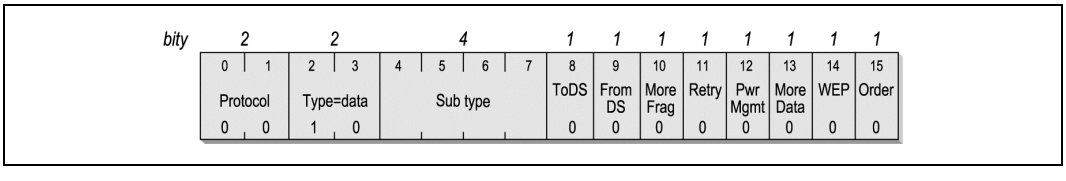
Ramki chronione przez WEP nie są nowym typem ramek. Kiedy ramka zostaje poddana działaniu mechanizmu WEP, bit WEP w polu Frame Control zostaje ustawiony na 1, a pole Frame Body (treść ramki) rozpoczyna się od nagłówka WEP opisanego w rozdziale 5.

Ramki kontrolne

Ramki kontrolne pełnią funkcje pomocnicze podczas dostarczania ramek danych. Zarządzają one dostępem do nośnika bezprzewodowego (ale nie samym nośnikiem) i są odpowiedzialne za niezawodność warstwy MAC.

Wspólne pole Frame Control

Wszystkie ramki kontrolne posługują się tym samym polem Frame Control. Pokazano je na rysunku 4.12.



Rysunek 4.12. Pole Frame Control w ramkach kontrolnych

Protocol version

Na rysunku 4.12 pole Protocol widoczne jest jako 0, ponieważ obecnie jest to jedyna istniejąca wersja. W przyszłości mogą pojawić się również inne wersje.

Type

Ramkom kontrolnym przypisany jest identyfikator Type (typ) o wartości 01. Z definicji wszystkie ramki kontrolne posługują się tym identyfikatorem.

Subtype

To pole wskazuje na Subtype (podtyp) transmitowanej ramki kontrolnej.

ToDS, FromDS

Ramki kontrolne arbitrażowo przyznają dostęp do nośnika bezprzewodowego i z tego powodu ich miejscem pochodzenia mogą być jedynie stacje bezprzewodowe. System dystrybucyjny nie wysyła ramek kontrolnych ani nie otrzymuje ich, a więc bity ToDS i FromDS są zawsze ustawione na 0.

More Fragments

Ramki kontrolne nie podlegają fragmentacji, a więc bit More Fragments, wskazujący na istnienie kolejnych fragmentów, jest zawsze ustawiony na 0.

Retry

Ramki kontrolne nie są ustawiane w kolejce do retransmisji, tak jak ramki zarządzające lub ramki danych, a więc bit Retry (ponowienie próby) jest zawsze ustawiony na 0.

Power Management

Bit Power Management jest ustawiony na taką wartość, która będzie wskazywać, w jakim trybie pod względem zarządzania energią (*power management*) będzie się znajdować stacja po ukończeniu bieżącej wymiany ramek.

More Data

Bit More Data jest wykorzystywany wyłącznie w ramkach zarządzających i ramkach danych, a więc w ramkach kontrolnych bit ten jest zawsze ustawiony na 0.

WEP

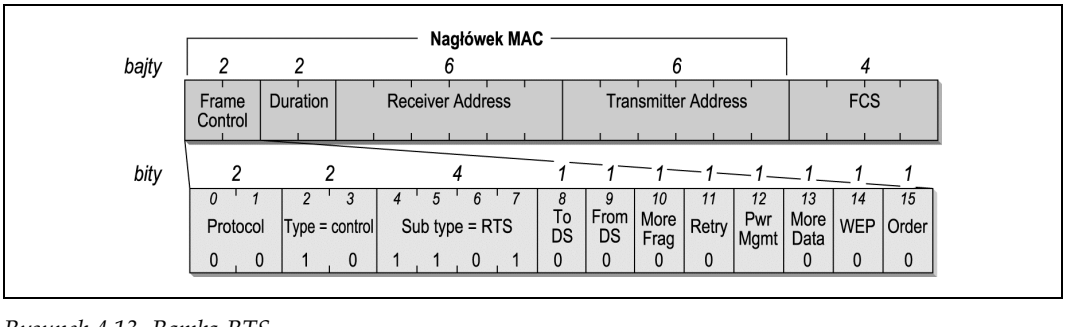
Ramki kontrolne nie mogą być kodowane za pomocą WEP, stosowanego wyłącznie do ramek danych i zapytań o skojarzenie (*association request*). Tym samym w ramkach kontrolnych bit WEP jest zawsze ustawiony na 0.

Order

Ramki kontrolne są komponentami operacji atomowych wymian ramek i z tego powodu nie mogą być transmitowane poza kolejnością. W związku z tym bit Order jest ustawiony na wartość 0.

RTS — ramka Request To Send

Ramki RTS służą do uzyskiwania kontroli nad nośnikiem w celu transmisji „dużych" ramek, przy czym wielkość tych ramek zdefiniowana została przez próg RTS w sterowniku karty sieciowej. Dostęp do nośnika może być rezerwowany tylko dla ramek typu unicast; ramki typu broadcast i multicast są zwyczajnie transmitowane. Format ramki RTS został pokazany na rysunku 4.13. Tak jak w przypadku wszystkich ramek kontrolnych, ramka RTS w całości jest nagłówkiem. W treści ramki nie transmituje się żadnych danych, a zaraz za nagłówkiem znajduje się pole FCS.



Rysunek 4.13. Ramka RTS

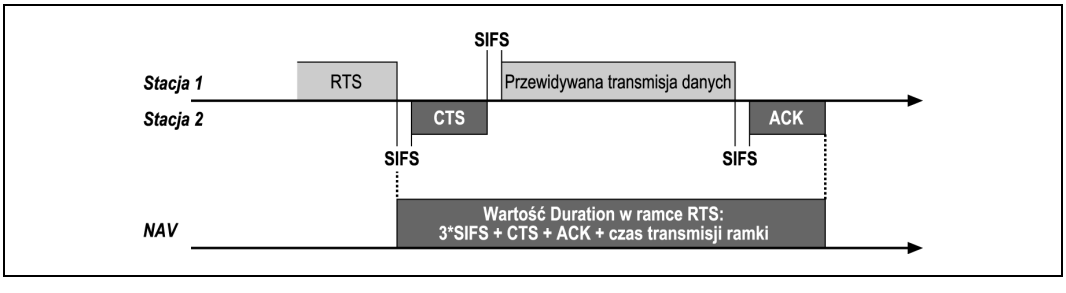
Na nagłówek MAC ramki RTS składają się cztery pola.

Frame Control

W polu Frame Control nie można się doszukać niczego wyjątkowego. Podtyp ramki jest ustawiony na wartość 1011, co wskazuję, że jest to ramka RTS, ale poza tym charakteryzuje się wszystkimi innymi polami typowymi dla pozostałych ramek kontrolnych. (Najbardziej znaczące bity w specyfikacji 802.11 znajdują się na końcu pól, co oznacza, że bit 7. jest najważniejszym bitem w polu Subtype).

Duration

Ramka RTS podejmuje próby rezerwowania nośnika na pełną wymianę ramek i z tego względu nadawca ramki RTS oblicza czas potrzebny na przesłanie sekwencji wymiany ramek po zakończeniu ramki RTS. Cała wymiana, która została przedstawiona na rysunku 4.14, wymaga czasu równego trzem okresom SIFS, długości nadania jednego CTS oraz ostatniego ACK plus czas potrzebny na transmisję ramki lub pierwszego jej fragmentu. (Wiązki fragmentacyjne posługują się następującymi po sobie fragmentami w celu uaktualniania pola Duration). Liczba mikrosekund potrzebna na transmisję jest obliczana i umieszczana w polu Duration. Jeśli wynik jest wartością ułamkową, zostaje zaokrąglony do następnej mikrosekundy.



Rysunek 4.14. Pole Duration w ramce RTS

Address 1: Receiver Address (adres odbiornika)

Pole to wskazuje stację, która jest zamierzonym adresatem dużej ramki.

Address 2: Transmitter Address (adres nadajnika)

Pole to wskazuje nadawcę ramki *RTS*.

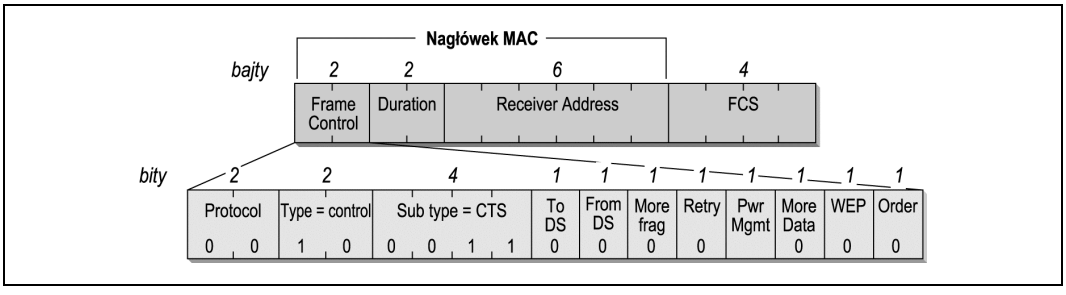
CTS — ramka Clear To Send

Ramki CTS są odpowiedziami na ramki RTS. Ich format pokazano na rysunku 4.15.

Na nagłówek MAC ramki CTS składają się trzy pola.

Frame Control

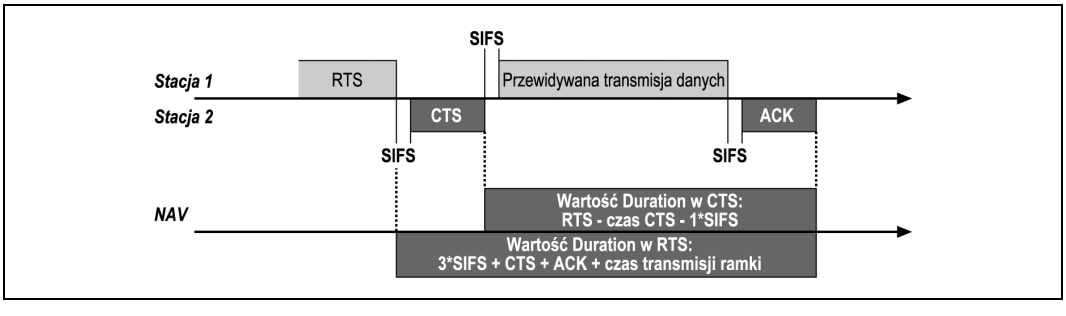
Podtyp ramki jest ustawiony na wartość 1100, która wskazuje, że jest to ramka CTS.



Rysunek 4.15. Ramka CTS

Duration

Nadawca ramki CTS posługuje się wartością pola Duration ramki RTS do obliczeń swojego czasu trwania. Ramki RTS rezerwują nośnik dla całej wymiany RTS-CTS-ramka-ACK. Gdy nadchodzi kolej na transmisję ramki CTS, do wysłania pozostają jedynie ramka lub jej fragment oraz potwierdzenie. Nadawca ramki CTS odejmuje od okresu trwania ramki RTS czas potrzebny do wysłania ramki CTS oraz okres SIFS poprzedzający CTS, a wynik tych obliczeń umieszcza w polu Duration. Rysunek 4.16 ilustruje zależność między wartościami pola Duration ramki CTS i ramki RTS.



Rysunek 4.16. Pole Duration ramki CTS

Address 1: Receiver Address (adres odbiornika)

Odbiorcą ramki CTS jest nadajnik ramki RTS, a więc MAC kopiuje adres nadajnika ramki RTS i zapisuje jako adres odbiornika ramki CTS.

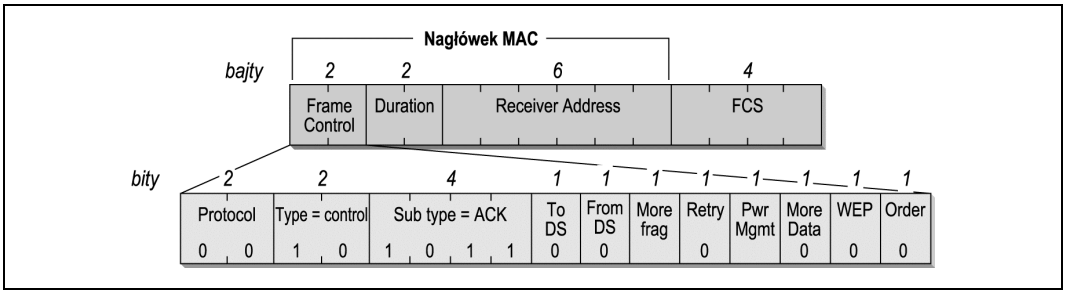
Ramki potwierdzenia — ACK

Ramki ACK są używane do wysyłania pozytywnych potwierdzeń wymaganych przez warstwę MAC i stosuje się je przy każdej transmisji danych, w tym w zwykłych transmisjach; ramki te są poprzedzane przez uzgodnienie RTS/CTS i ramki fragmentowane (patrz rysunek 4.17).

Na nagłówek MAC ramki ACK składają się trzy pola.

Frame Control

Podtyp ramki jest ustawiony na wartość 1101, która wskazuje, że jest to ramka ACK.

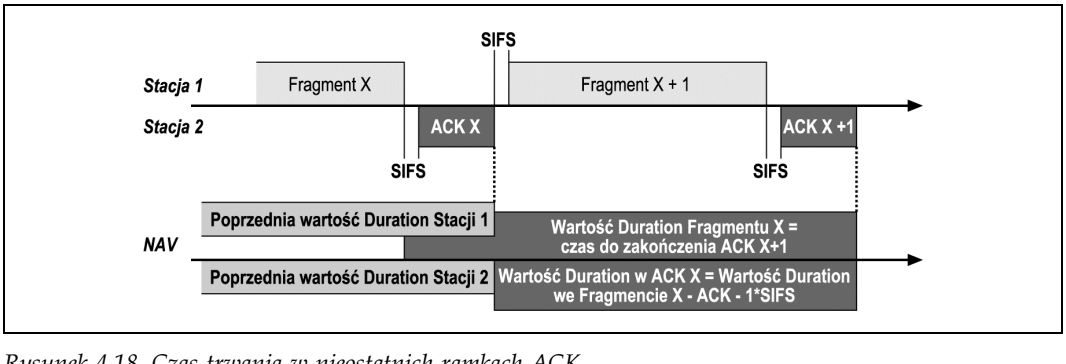


Rysunek 4.17. Ramka ACK

Duration

Pole czasu trwania może być ustawione na jeden z dwóch sposobów w zależności od pozycji ACK w układzie wymiany ramek. Potwierdzenia ACK dla kompletnych ramek danych i ostatnich fragmentów w wiązce ustawiają pole Duration na 0. Nadawca danych wskazuje na koniec transmisji danych przez ustawienie bitu More Fragments w nagłówku Frame Control na wartość 0. Jeśli bit More Fragments wynosi 0, transmisję uznaje się za ukończoną i nie ma potrzeby utrzymania kontroli nad kanałem radiowym dla kolejnych transmisji. W związku z tym pole Duration zostaje ustawione na wartość 0.

Jeśli bit More Fragments wynosi 1, oznacza to, że wiązka fragmentacyjna jest w trakcie nadawania. Pole Duration zachowuje się wtedy tak samo jak w ramce CTS. Czas potrzebny do transmisji potwierdzenia ACK i jego odstępu SIFS jest odejmowany od okresu trwania w ostatnim transmitowanym fragmencie (patrz rysunek 4.18). Obliczanie czasu trwania w nieostatnich ramkach ACK przypomina obliczenia dla ramek CTS. Prawdę mówiąc, specyfikacja 802.11 ustawienia pola Duration w ramkach ACK określa jako *wirtualne CTS*.



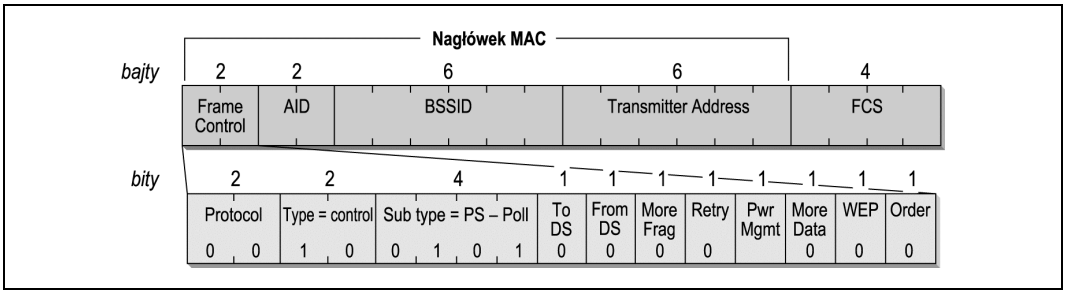
Rysunek 4.18. Czas trwania w nieostatnich ramkach ACK

Address 1: Receiver Address (adres odbiornika)

Adres odbiornika jest kopią adresu nadawcy ramki, której odbiór się potwierdza. Ze strony technicznej wygląda to następująco: adres jest kopiowany z pola Address 2 ramki otrzymującej potwierdzenie. Potwierdzenia są odpowiedzią na nakierowane ramki danych, ramki zarządzające oraz ramki PS-Poll.

Ramki Power-Save Poll (PS-Poll)

Kiedy stacja przenośna budzi się z trybu oszczędzania energii, wysyła ramkę PS-Poll do punktu dostępowego, by odebrać wszystkie ramki buforowane dla niej w okresie, gdy była nieaktywna. Format ramki PS-Poll przedstawia rysunek 4.19.



Rysunek 4.19. Ramka PS-Poll

Na nagłówek MAC ramki PS-Poll składają się cztery pola.

Frame Control

Podtyp ramki jest ustawiony na wartość 1010, która wskazuje, że jest to ramka PS-Poll.

AID — Association ID

Trzeci i czwarty bajt w nagłówku MAC ramka PS-Poll wykorzystuje nie na pole Duration, lecz na identyfikator AID. Jest to wartość numeryczna przypisywana przez punkt dostępowy w celu określenia skojarzenia. Umieszczenie AID w ramce pozwala punktowi dostępowemu znaleźć wszelkie ramki buforowane dla nowo obudzonej stacji przenośnej.

Address 1: BSSID

To pole zawiera BSSID dla BSS-u utworzonego przez punkt dostępowy, z którym nadawca jest obecnie skojarzony.

Address 2: Transmitter Address (adres nadajnika)

Jest to adres nadawcy ramki PS-Poll.

Association ID (AID)

W ramkach PS-Poll pole Duration/ID wypełnione jest raczej identyfikatorem AID, a nie wartością wykorzystywaną przez wirtualną funkcję rozpoznania stanu nośnika (*carrier-sensing*). Kiedy stacje przenośne łączą się z punktem dostępowym, punkt ten nadaje im wartość noszącą nazwę Association ID (AID) i mieszczącą się w zakresie od 1 do 2007. AID służy licznym zadaniom, które zostały opisane w tej książce.

Ramka PS-Poll nie zawiera informacji o czasie trwania, która umożliwia uaktualnienie wektora alokacji sieci NAV. Jednakże wszystkie stacje otrzymujące ramkę PS-Poll uaktualniają NAV za pomocą odstępu SIFS i czasu potrzebnego do transmisji potwierdzenia. Automatyczne uaktualnianie wektora NAV pozwala punktowi dostępowemu transmitować ACK z małym prawdopodobieństwem kolizji ze stacją przenośną.

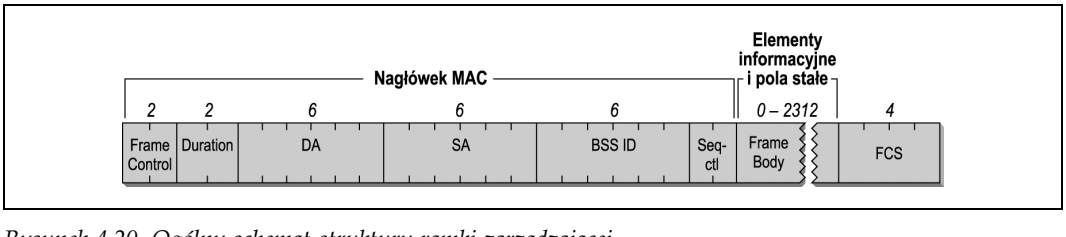
Ramki zarządzające

Zarządzanie stanowi pokaźną część specyfikacji 802.11. Opisuje ona kilka różnych typów ramek zarządzających stosowanych w usługach, które w sieciach przewodowych są operacjami łatwymi. W sieciach takich ustalenie tożsamości stacji sieciowej jest proste, ponieważ każde połączenie sieciowe wymaga pociągnięcia kabla z centralnej lokalizacji do nowej stacji roboczej. W wielu przypadkach tablice połączeń w szafie z okablowaniem przyspieszają instalację, jednak najważniejsza kwestia pozostaje niezmienna: nowe połączenia sieciowe powstają (są uwierzytelniane) po osobistej wizycie (osobistym logowaniu), w momencie gdy zakłada się nowe połączenie.

Aby rozwiązania w sieciach bezprzewodowych były równie komfortowe, muszą oferować pewne funkcje zarządzające. Standard 802.11 dzieli całą procedurę na trzy komponenty. Stacje przenośne, poszukując możliwości połączenia się z siecią, są zmuszone do zlokalizowania najpierw kompatybilnej sieci bezprzewodowej. (Dla sieci przewodowych etap ten wymaga zazwyczaj odnalezienia odpowiedniego gniazda w ścianie). Następnie sieć musi sprawdzić tożsamość stacji przenośnych, aby ustalić, czy stacja, która została uwierzytelniona, może połączyć się z siecią. (Odpowiednik tego kroku w sieciach przewodowych jest przeprowadzany przez samą sieć. Jeśli sygnały nie mogą opuścić kabla, uzyskanie fizycznego dostępu jest już w pewnym stopniu procesem uwierzytelniającym). Aż w końcu stacje przenośne muszą zostać skojarzone (powiązane) z punktem dostępowym, żeby otrzymać dostęp do przewodowego szkieletu sieci, co jest odpowiednikiem wpięcia kabla do sieci przewodowej.

Struktury ramek zarządzających

Ramki zarządzające przekazywane w sieciach bezprzewodowych posiadają strukturę pokazaną na rysunku 4.20.



Rysunek 4.20. Ogólny schemat struktury ramki zarządzającej

Nagłówek MAC jest taki sam we wszystkich ramkach zarządzających; nie zależy od podtypu ramki. Niektóre z ramek zarządzających posługują się treścią ramki do przesyłania informacji, które są charakterystyczne dla konkretnych podtypów.

Pola adresowe

Jak w przypadku wszystkich innych ramek, pierwsze pole adresowe reprezentuje adres docelowy ramki. Niektóre z ramek zarządzających służą do zatrzymania pewnych właściwości w granicach jednego BSS-u. Aby ograniczyć wpływ ramek zarządzających typu broadcast i multicast, po otrzymaniu ramki stacje sprawdzają jej identyfikator BSSID. Jedynie ramki typu broadcast i multicast z BSSID, z którym stacja jest w danej chwili skojarzona, są przekazywane do warstw zarządzających MAC. Jedynym wyjątkiem od tej reguły są ramki Beacon, które informują o obecności sieci bezprzewodowej.

BSSID jest nadawany w podobny sposób. Punkty dostępowe posługują się adresem MAC interfejsu sieci bezprzewodowej jako identyfikatorem BSSID. Stacje przenośne przyjmują BSSID punktu dostępowego, z którym są obecnie skojarzone. Stacje w sieci IBSS używają BSSID-u losowo wygenerowanego przez BSS. Istnieje jeden wyjątek od reguły: ramki wysyłane przez stację przenośną szukające konkretnej sieci mogą posługiwać się BSSID sieci, której szukają, lub wykorzystać BSSID typu broadcast, żeby odnaleźć wszystkie stacje znajdujące się w sąsiedztwie.

Obliczenia czasu trwania

Ramki zarządzające stosują pole Duration w taki sam sposób jak inne ramki.

1. Wszystkie ramki, które są wysyłane w okresie bez rywalizacji o dostęp, ustawiają czas trwania (*Duration*) na 32 768.
2. Ramki transmitowane podczas okresów z rywalizacją o dostęp, posługujące się jedynie DCF, stosują pole Duration do blokowania dostępu do nośnika, by umożliwić zakończenie atomowych wymian ramek.
   a) Jeśli ramka jest typu broadcast lub multicast (adres docelowy obejmuje grupę adresatów), pole Duration jest ustawione na wartość 0. Ramki te nie wymagają potwierdzenia, a więc wektor NAV nie jest potrzebny do blokowania dostępu do nośnika.
   b) Jeśli nieostatni fragment jest częścią wymiany wieloramkowej, pole Duration ustawione jest na liczbę mikrosekund potrzebną na trzy odstępy SIFS, następny fragment i jego potwierdzenie.
   c) Fragmenty ostatnie w pole Duration wpisują wartość, która jest czasem wymaganym dla wysłania jednego potwierdzenia i jednego odstępu SIFS.

Treść ramki

Ramki zarządzające charakteryzują się dość dużą elastycznością. Większość danych zawartych w treści zasadniczej ramki (*Frame Body*) zajmuje pola o stałej długości noszące

nazwę *pól stałych* (*Fixed Fields*) oraz pola o zróżnicowanej długości noszące nazwę *elementów informacyjnych* (*Information Elements*). Elementy informacyjne są blobami[2] danych, charakteryzującymi się różnymi rozmiarami. Każdy pakiet danych jest wyposażony w etykietkę z numerem typu i rozmiarem. Jasne jest, że element informacyjny konkretnego typu wyposażony jest w pole danych interpretowane w konkretny sposób. Nowe elementy informacyjne mogą być definiowane przez nowsze nowelizacje specyfikacji 802.11. Rozwiązania, które wyprzedzają w czasie nowelizacje, mogą ignorować nowsze elementy. Stare implementacje opierają się na sprzęcie kompatybilnym wstecz i często okazuje się, że nie mogą one podłączyć się do sieci opartych na nowszych standardach. Szczęśliwym trafem istnieje możliwość wyłączenia nowych opcji, gdy przeszkadzają one w osiągnięciu zgodności sprzętowej.

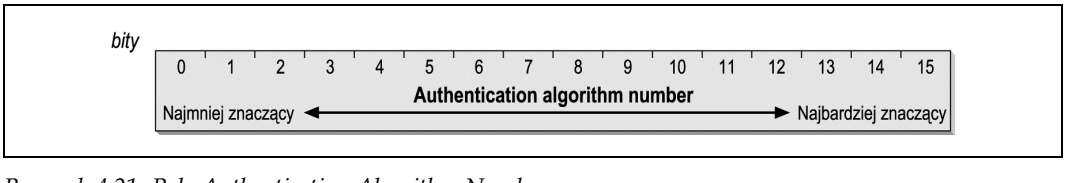
W tej części rozdziału przedstawione zostaną pola stałe i elementy informacyjne będące częściami składowymi ramek zarządzających oraz sposób ich zestawienia ze sobą w tychże ramkach. Standard 802.11 precyzuje kolejność, w jakiej mają się pojawiać elementy informacyjne, przy czym nie wszystkie elementy są obowiązkowe. Niniejsza książka prezentuje każdą część składową ramek w konkretnej kolejności, a rozważania na temat konkretnych podtypów zwracają uwagę na to, które z części rzadko występują, a które wzajemnie się wykluczają.

Komponenty o stałej długości

W ramkach zarządzających pojawia się dziesięć pól o stałej długości. Pola te są często po prostu określane mianem *pól* w odróżnieniu od elementów informacyjnych, charakteryzujących się zmienną długością.

Pole Authentication Algorithm Number

Dwa bity są przeznaczone na pole Authentication Algorithm Number (numer algorytmu uwierzytelniającego), pokazane na rysunku 4.21. Pole to identyfikuje typ uwierzytelnienia stosowany w procesie uwierzytelniania. (Proces uwierzytelniania został szczegółowo opisany w rozdziale 7.). Dopuszczalne wartości dla tego pola przedstawia tabela 4.3. Aktualnie tylko dwie wartości zostały zdefiniowane, a pozostałe są zarezerwowane dla przyszłych procesów standaryzacyjnych.



Rysunek 4.21. Pole Authentication Algorithm Number

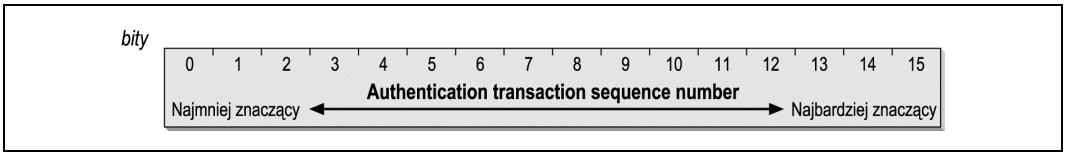
[2] Termin „blob" sam w sobie znaczy tyle co kropla, kula i nie został pierwotnie ukuty jako skrót od Dużego Obiektu Binarnego („Binary Large Object", czy „Basic Large Object"), ale zaczerpnięty z filmu klasy „B" noszącego tytuł „The Blob", w którym Blob był bezkształtną istotą z kosmosu, która zjadała duże połacie Stanów Zjednoczonych — *przyp. tłum.*

Tabela 4.3. Wartości pola Authentication Algorithm Number

Wartość	Znaczenie
0	uwierzytelnienie typu Open System
1	uwierzytelnienie typu Shared Key
2 – 65 535	zarezerwowane

Authentication Transaction Sequence Number

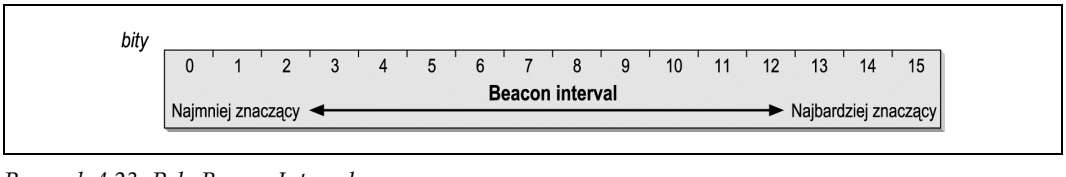
Uwierzytelnianie jest procesem wieloetapowym, który składa się ze składanego przez punkt dostępowy wezwania do podania tożsamości (*challenge*) i odpowiedzi dawanej przez stację przenośną podejmującą próbę skojarzenia się z punktem. Authentication Transaction Sequence Number pokazany na rysunku 4.22 jest dwubitowym polem wykorzystywanym do śledzenia procesu przez wymianę ramek zmierzającą do uzyskania uwierzytelniania. Przyjmuje ono wartości od 1 do 65 535, natomiast nigdy nie zostaje ustawione na wartość 0. Zastosowanie tego pola zostało opisane w rozdziale 7.



Rysunek 4.22. Pole Authentication Transaction Sequence Number

Beacon Interval

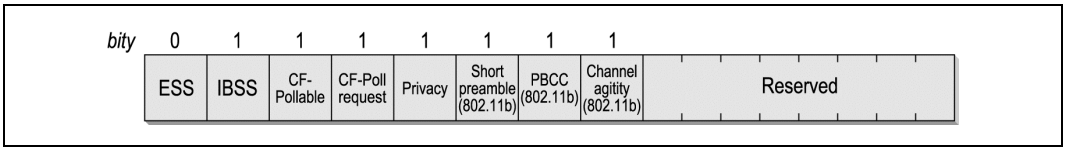
Transmisje typu Beacon w regularnych odstępach czasu komunikują o istnieniu sieci 802.11. Ramki Beacon niosą informację o parametrach BSS-u i ramkach buforowanych przez punkty dostępowe, tak więc stacje przenośne muszą słuchać tych komunikatów. Beacon Interval (odstęp Beacon) pokazany na rysunku 4.23 jest 16-bitowym polem wskazującym liczbę *jednostek czasu* pomiędzy transmisjami typu Beacon. Jedna jednostka czasu (*Time Unit — TU*) to 1 024 mikrosekund (µs), co stanowi około 1 milisekundy. Jednostki czasu bywają nazywane kilomikrosekundami w różnych źródłach (Kµs lub kµs). Najczęściej odstęp Beacon jest ustawiony na 100 jednostek czasu, co odpowiada odstępowi między transmisjami typu Beacon o długości około 100 milisekund lub 0,1 sekundy.



Rysunek 4.23. Pole Beacon Interval

Pole Capability Information

16-bitowe pole Capability Information pokazane na rysunku 4.24 jest wykorzystywane w transmisjach typu Beacon w celu informowania o możliwościach (*capability*) sieci. Pole



Rysunek 4.24. Pole Capability Information

to jest stosowane również w ramkach Probe Request i Probe Response. W polu Capability Information każdy bit występuje jako flaga reklamująca konkretną funkcję sieci. Stacje posługują się informacją o możliwościach sieci do określania, czy są w stanie obsługiwać wszystkie funkcje obowiązujące w BSS. Stacje, które nie posiadają wszystkich funkcji wymienionych w tym polu, nie otrzymują zezwolenia na włączenie się do sieci.

ESS/IBSS

Oba te bity wzajemnie się wykluczają. Punkty dostępowe ustawiają wartość pola ESS na 1 i pola IBSS na 0, żeby wskazać, że punkt dostępowy jest częścią sieci stacjonarnej. Stacje znajdujące się w sieci IBSS ustawiają pole ESS na wartość 0, a pole IBSS na 1.

Privacy

Ustawienie bitu Privacy na wartość 1 wymaga użycia protokołu WEP dla zachowania poufności. W sieciach stacjonarnych nadajnikiem jest punkt dostępowy. W sieciach IBSS transmisja Beacon musi być przeprowadzana przez stację znajdującą się w IBSS.

Short preamble

Pole to zostało dodane do specyfikacji 802.11b, by obsługiwać warstwę fizyczną w szybkiej technologii DSSS. Ustawienie go na wartość 1 wskazuje, że sieć posługuje się krótką preambułą w sposób opisany w rozdziale 10. Zero oznacza, że opcja ta nie jest wykorzystywana i jest zabroniona w sieci BSS.

PBCC

Pole PBCC (*Packet Binary Convolution Coding*) zostało dodane do specyfikacji 802.11b, by obsługiwać warstwę fizyczną w szybkiej technologii DSSS. Kiedy jego wartość jest ustawiona na 1, wskazuje ono, że sieć posługuje się schematem modulacji PBCC, opisanym w rozdziale 10. Zero oznacza, że opcja ta nie jest wykorzystywana i jest zabroniona w sieci BSS.

Channel Agility

Pole to zostało dodane do specyfikacji 802.11b, by obsługiwać warstwę fizyczną w szybkiej technologii DSSS. Kiedy jego wartość jest ustawiona na 1, wskazuje ono, że sieć posługuje się opcją Channel Agility, opisaną w rozdziale 10. Zero oznacza, że opcja ta nie jest wykorzystywana i jest zabroniona w sieci BSS.

Bity Contention-free polling

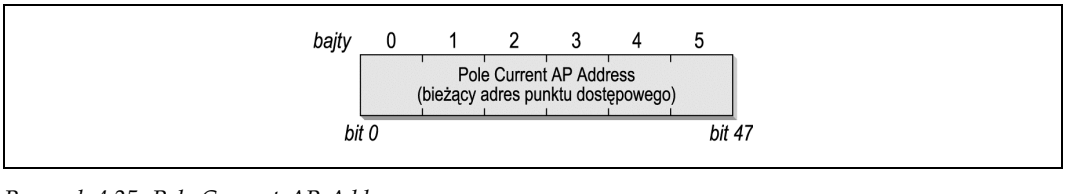
Stacje i punkty dostępowe posługują się tymi dwoma bitami jako etykietkami. Znaczenia tych etykiet zostały przedstawione w tabeli 4.4.

Tabela 4.4. Interpretacja bitów odpytywania (polling) w Capability Information

CF-Pollable	CF-Poll Request	Interpretacja
Zastosowanie w stacjach		
0	0	Stacja nie obsługuje odpytywania.
0	1	Stacja obsługuje odpytywanie, ale nie ubiega się o miejsce na liście odpytywań.
1	0	Stacja obsługuje odpytywanie i ubiega się o miejsce na liście odpytywań.
1	1	Stacja obsługuje odpytywanie i ubiega się o niewciąganie jej na listę odpytywań (w rezultacie stacja jest traktowana, jakby nie obsługiwała operacji bez rywalizacji o dostęp).
Zastosowanie w punktach dostępowych		
0	0	Punkt dostępowy nie wdraża funkcji koordynacji punktu.
0	1	Punkt dostępowy używa PCF do dostarczania ramek, ale nie obsługuje odpytywania.
1	0	Punkt dostępowy używa PCF do dostarczania ramek i odpytywania.
1	1	Zarezerwowane, nieużywane.

Pole Current AP Address

Stacje przenośne posługują się polem Current AP Address (adres bieżącego punktu dostępowego), pokazanym na rysunku 4.25, żeby podać adres MAC punktu dostępowego, z którym są skojarzone. Pole to ma na celu ułatwiać uzyskanie skojarzeń i skojarzeń ponownych. Stacje transmitują adres punktu, który był odpowiedzialny za ostatnie skojarzenie z siecią. Kiedy skojarzenie zostanie nawiązane z innym punktem dostępowym, pole to może przenieść skojarzenie i odebrać wszystkie ramki buforowane.

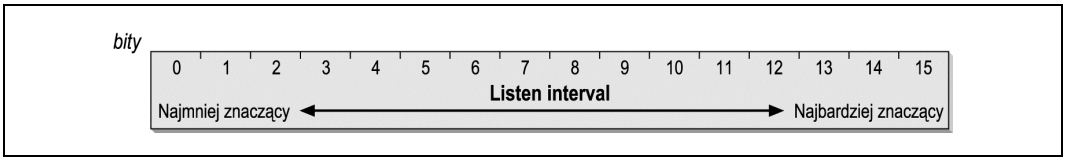


Rysunek 4.25. Pole Current AP Address

Listen Interval

W wydłużenia żywotności baterii stacje wyłączają anteny w bezprzewodowych interfejsach sieciowych. Gdy stacje znajdują się w stanie uśpienia, punkty dostępowe muszą dla nich buforować ramki. Uśpione stacje budzą się w pewnych odstępach czasu i słuchają ogłoszeń o ruchu sieciowym, co pozwala im ocenić, czy punkty dostępowe mają dla nich

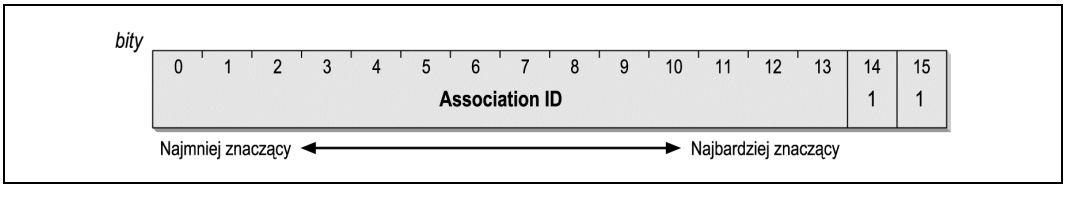
jakieś buforowane ramki. Kiedy stacje kojarzą się z punktem dostępowym, częścią zapisanych danych jest *Listen Interval*. Jest on liczbą odstępów typu Beacon, przez długość których stacje czekają, zanim ponownie rozpoczną słuchanie ramek Beacon. Listen Interval pokazany na rysunku 4.26, pozwala stacjom przenośnym poinformować punkt dostępowy, jak długo musi zachowywać dla nich buforowane ramki. Dłuższe odstępy Listen Interval wymagają większej pamięci punktu dostępowego potrzebnej do buforowania ramek. Punkty dostępowe mogą wykorzystać tę funkcję do oceny wymaganych zasobów i odrzucić skojarzenia wymagające zbyt dużych zasobów. Odstępy Listen Interval zostały omówione w rozdziale 7.



Rysunek 4.26. Pole Listen Interval

Association ID

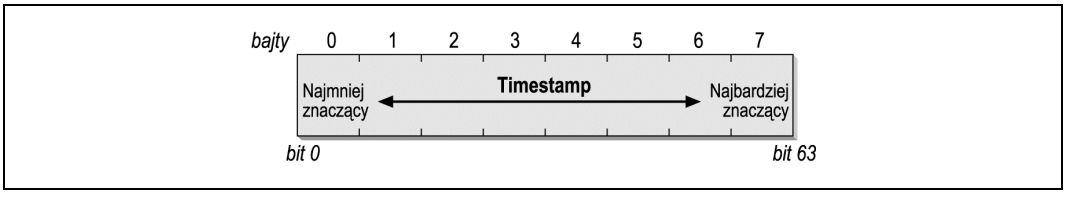
Association ID, pokazane na rysunku 4.27, jest polem 16-bitowym. Kiedy stacje kojarzą się z punktem dostępowym, zostaje im przypisany numer identyfikacyjny powiązania, pomocny w realizacji funkcji kontrolnych i zarządzania. Mimo że do tworzenia Association ID dostępnych jest 14 bitów, AID to liczby z zakresu od 1 do 2 007. Dla zachowania kompatybilności z polem Duration/ID w nagłówku MAC dwa najważniejsze bity są ustawione na 1.



Rysunek 4.27. Pole Association ID

Pole Timestamp

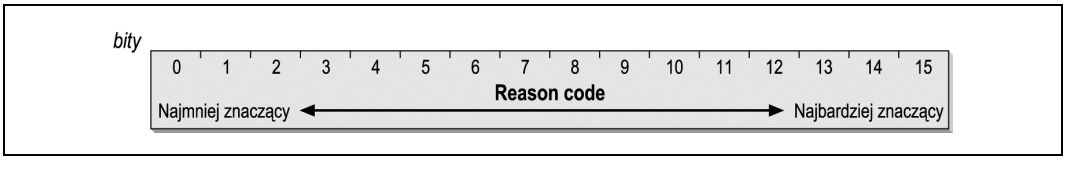
Pole Timestamp, pokazane na rysunku 4.28, umożliwia synchronizację między stacjami w jednej sieci BSS. Główny czasomierz w BSS co jakiś czas informuje, jak długo jest już aktywny. Czas ten podaje w mikrosekundach. Kiedy licznik osiąga swoją maksymalną wartość, zeruje się. (Wyzerowanie się licznika jest bardzo mało prawdopodobne, kiedy weźmiemy pod uwagę okres, jaki musiałby minąć, by doprowadzić do wyzerowania się 64-bitowego licznika. W okresie ponad 580 000 lat, zanim ten licznik się wyzeruje, z całą pewnością zdąży powstać niejeden program korekcyjny).



Rysunek 4.28. Pole Timestamp

Pole Reason Code

Stacje posiadają możliwość wysyłania ramek Disassociation (zerwanie skojarzenia) lub Deauthentication (zerwanie uwierzytelnienia) w odpowiedzi na ruch sieciowy, kiedy nadawca w nieodpowiedni sposób włączył się do sieci. Częścią takiej ramki jest 16-bitowe pole Reason Code, pokazane na rysunku 4.29, a mające na celu informowanie, co nadawca zrobił w nieodpowiedni sposób. Tabela 4.5 pokazuje, dlaczego generowane są niektóre pola Reason Code. Dla pełnego zrozumienia zastosowania Reason Code wymagane jest poznanie różnych klas ramek i stanów stacji bezprzewodowych; to zagadnienie zostało przedstawione w podrozdziale „Transmisja ramek oraz stany skojarzenia i uwierzytelnienia".



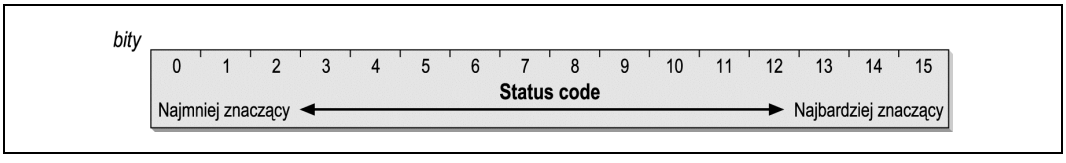
Rysunek 4.29. Pole Reason Code

Tabela 4.5. Reason Code

Kod	Przyczyna
0	Zarezerwowane; nieużywane.
1	Nieokreślone.
2	Wcześniejsze uwierzytelnienie nie jest ważne.
3	Stacja opuściła BSS lub ESS i straciła uwierzytelnienie.
4	Upłynął czas dozwolonej nieaktywności i zerwano skojarzenie ze stacją.
5	Zerwanie skojarzenia w wyniku niewystarczających zasobów punktu dostępowego.
6	Nieprawidłowy typ lub podtyp ramki otrzymany od stacji bez uwierzytelnienia.
7	Nieprawidłowy typ lub podtyp ramki otrzymany od stacji bez skojarzenia.
8	Stacja opuściła BSS lub ESS i straciła skojarzenie.
9	Wymagane jest skojarzenie lub zerwanie skojarzenia, zanim uwierzytelnianie zostanie zakończone.
10 – 65 535	Zarezerwowane; nieużywane.

Pole Status Code

Pole Status Code informuje o udanej lub nieudanej operacji. W polu tym, pokazanym na rysunku 4.30, znajduje się 0, gdy operacja ukończona została pomyślnie i wartość inna niż zero — w przypadku porażki. Tabela 4.6 pokazuje Status Code, które poddane zostały standaryzacji.



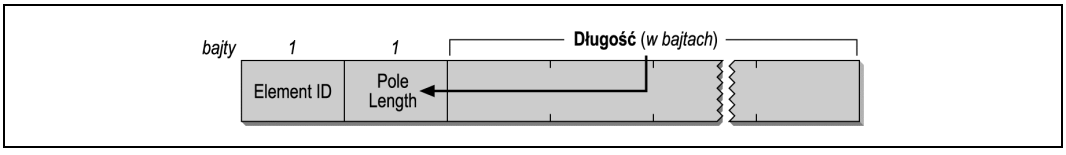
Rysunek 4.30. Pole Status Code

Tabela 4.6. Status Code

Kod	Wyjaśnienie kodu
0	Operacja zakończona pomyślnie.
1	Nieokreślony błąd.
2 – 9	Zarezerwowane; nieużywane.
10	Żądany zestaw możliwości jest zbyt obszerny i nie może zostać przyjęty.
11	Odmowa ponownego skojarzenia; poprzednie skojarzenie nie może zostać zidentyfikowane lub przeniesione.
12	Odmowa skojarzenia z powodu nieokreślonego w standardzie 802.11.
13	Żądany algorytm uwierzytelniania nie jest obsługiwany.
14	Nieoczekiwany numer sekwencji uwierzytelniania.
15	Odrzucenie uwierzytelnienia; niepomyślna odpowiedź na sygnał wezwania (*challenge*).
16	Odrzucenie uwierzytelnienia; kolejna ramka w sekwencji nie pojawiła się w oczekiwanym oknie.
17	Odmowa skojarzenia; punkt dostępowy ma ograniczone zasoby.
18	Odmowa skojarzenia; stacja przenośna nie obsługuje wszystkich szybkości transmisji danych wymaganych przez BSS.
19 (802.11b)	Odmowa skojarzenia; stacja przenośna nie obsługuje opcji Short Preamble.
20 (802.11b)	Odmowa skojarzenia; stacja przenośna nie obsługuje opcji modulowania typu PBCC.
21 (802.11b)	Odmowa skojarzenia; stacja przenośna nie obsługuje opcji Channel Agility.
22 – 65 535	Zarezerwowane dla przyszłych prac standaryzacyjnych.

Elementy informacyjne ramek zarządzających

Elementy informacyjne są dowolnej długości komponentami ramek zarządzających. Standardowy element informacyjny posiada numer ID, długość oraz komponent o dowolnej długości, co pokazano na rysunku 4.31. Standardowe wartości dla numeru ID elementu przedstawione zostały w tabeli 4.7.



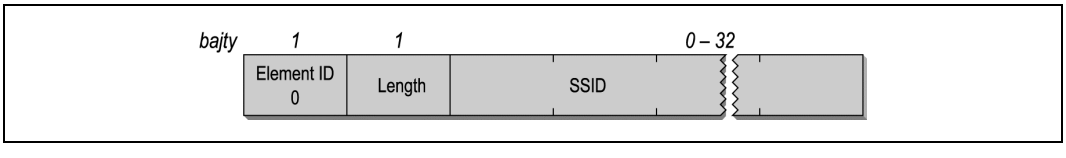
Rysunek 4.31. Element informacyjny ramki zarządzającej

Tabela 4.7. Elementy informacyjne

ID elementu	Nazwa
0	Service Set Identity (SSID)
1	obsługiwane szybkości transmisji
2	FH Parameter Set
3	DS Parameter Set
4	CF Parameter Set
5	TIM (Traffic Indication Map)
6	IBSS Parameter Set
7 – 15	zarezerwowane; nieużywane
16	treść wezwania (*challenge*).
17 – 31	zarezerwowane dla rozszerzenia tekstowego wezwania
32 – 255	zarezerwowane; nieużywane

Service Set Identity (SSID)

Osoby zarządzające sieciami są jedynie ludźmi i zazwyczaj wolą pracować na literach, liczbach i nazwach zamiast na 48-bitowych identyfikatorach. Sieci bezprzewodowe w najszerszym sensie są albo ESS-ami (*Extended Service Set*), albo niezależnymi BSS-ami (*Basic Service Set*). SSID (identyfikator zestawu sieciowego), pokazany na rysunku 4.32, daje zarządcom sieci możliwość przypisania identyfikatora do zestawu usług. Stacje chcące przyłączyć się do sieci mogą przeszukiwać nośnik w celu znalezienia dostępnych sieci i połączyć się z siecią o konkretnym SSID. SSID jest taki sam dla wszystkich zestawów BSS wchodzących w skład tego samego zestawu ESS.



Rysunek 4.32. Element informacyjny Service Set Identity

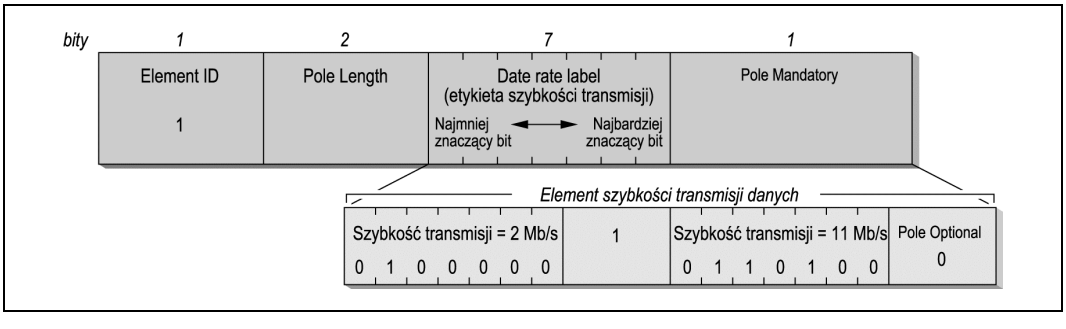
W niektórych dokumentacjach o SSID mówi się: *nazwa sieci*, ponieważ administratorzy sieci często przypisują mu ciąg znaków literowych. Większość produktów wymaga, by był to mało znaczący, zakończony zerem ciąg znaków systemu ASCII. We wszystkich przypadkach długość SSID mieści się w zakresie od 0 do 32 bajtów. Identyfikator z zerowym

bajtem to przypadek szczególny noszący nazwę *SSID typu broadcast*, który jest stosowany wyłącznie w ramkach Probe Request, kiedy stacja podejmuje próbę odkrycia wszystkich sieci bezprzewodowych znajdujących się w jej zasięgu.

Element informacyjny Supported Rates

Kilka szybkości transmisji danych zostało zatwierdzonych jako standardy sieci bezprzewodowych. Element informacyjny Supported Rates (obsługiwane szybkości transmisji) pozwala sieci 802.11 na określenie szybkości transmisji danych, które ona obsługuje. Kiedy stacje przenośne chcą połączyć się z siecią, sprawdzają używane w niej szybkości transmisji danych. Niektóre szybkości są obowiązkowe i muszą być obsługiwane przez stacje przenośne, pozostałe są opcjonalne.

Element informacyjny Supported Rates pokazano na rysunku 4.33. Składa się on z ciągu bajtów. Każdy bajt przeznacza siedem mniej ważnych bitów na szybkości transmisji; bit najważniejszy informuje, czy dana szybkość jest obowiązkowa. Właśnie te obowiązkowe szybkości są kodowane z najważniejszym bitem ustawionym na wartość 1, a szybkości opcjonalne mają w tym miejscu 0. W elemencie informacyjnym można zakodować do ośmiu szybkości transmisji danych.



Rysunek 4.33. Element informacyjny Supported Rates

W pierwszej nowelizacji specyfikacji 802.11 siedem bitów kodowało szybkość transmisji jako wielokrotność 500 kb/s. Nowa technologia, zwłaszcza osiągnięcia HIPERLAN instytutu ETSI[3], wymaga zmiany tej zasady. Kiedy siedem bitów służy uzyskaniu wielokrotności 500 kb/s, maksymalną szybkością, jaka może być zakodowana jest 63,5 Mb/s. Badania naukowe i rozwojowe nad technologiami stosowanymi w bezprzewodowych sieciach LAN sprawiły, że szybkość ta stanie się osiągalna już w najbliższej przyszłości. W reakcji na ten postęp IEEE zmienił interpretację z wielokrotności 500 kb/s na zwykłą etykietę w standardzie 802.11b. Wcześniej znormalizowane szybkości transmisji otrzymywały etykiety odpowiadające wielokrotności 500 kb/s, ale przyszłe standardy mogą posługiwać się jakąkolwiek wartością. Obecnie wykorzystywane wartości przedstawione zostały w tabeli 4.8.

[3] European Telecommunications Standards Institute — *przyp. tłum.*

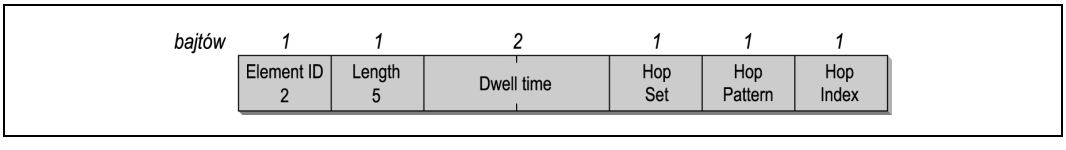
Tabela 4.8. Etykiety Supported Rates

Wartość binarna	Szybkość
2	1 Mb/s
4	2 Mb/s
11	5,5 Mb/s
22	11 Mb/s

Rysunek 4.33 pokazuje przykładowe szyfrowanie dwóch szybkości transmisji danych. Usługa 2 Mb/s jest obowiązkowa, natomiast usługa 11 Mb/s jest również możliwa. Jest to zakodowane jako szybkość obowiązkowa (w polu Mandatory) 2 Mb/s i opcjonalna (w polu Optional) 11 Mb/s.

FH Parameter Set

Element informacyjny FH Parameter Set, pokazany na rysunku 4.34, zawiera wszystkie parametry konieczne do przyłączenia się do sieci bezprzewodowej stosującej rozpraszanie skokowe (*frequency hopping — FH*).



Rysunek 4.34. Element informacyjny FH Parameter Set

FH Parameter Set ma cztery pola, które w jednoznaczny sposób określają sieć bezprzewodową opartą na rozpraszaniu skokowym. W rozdziale 10. szczegółowo opiszemy te identyfikatory.

Dwell Time

Sieci bezprzewodowe oparte na rozpraszaniu skokowym przeskakują z kanału na kanał. Okres czasu spędzony na każdym kanale w sekwencji skokowej nosi nazwę *dwell time*. Wyraża się go w jednostkach czasu (TU).

Hop Set

Kilka wzorów skoków zostało zdefiniowanych przez warstwę fizyczną FH sieci 802.11. Pole to, będące pojedynczym bajtem, wskazuje zestaw stosowanych wzorów skoków.

Hop Pattern

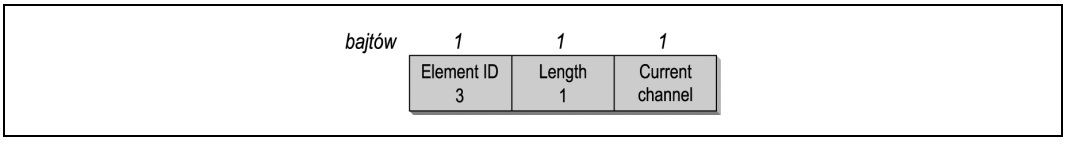
Z zestawu stacje wybierają jeden wzór skoków. Pole to, również będące pojedynczym bajtem, wskazuje stosowany wzór skoków.

Hop Index

Każdy wzór składa się z długiej sekwencji skoków między kanałami. Pole to, będące pojedynczym bajtem, wskazuje obecny punkt w sekwencji.

DS Parameter Set

Sieci bezprzewodowe stosujące rozpraszanie sekwencyjne (*direct sequence — DS*) posiadają tylko jeden parametr: numer kanału używanego przez sieć. Charakteryzujące się wysoką szybkością sieci z systemem dystrybucyjnym posługują się tymi samymi kanałami, a więc mogą wykorzystywać identyczny zestaw parametrów. Numer kanału jest zakodowany jako pojedynczy bajt, tak jak to pokazano na rysunku 4.35.

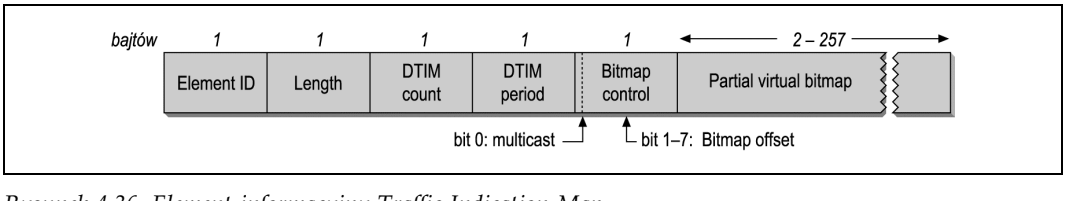


Rysunek 4.35. Element informacyjny DS Parameter Set

Element TIM

Punkty dostępowe buforują ramki dla stacji przenośnych znajdujących się akurat w trybie uśpienia, kiedy oszczędzają energię. Co jakiś czas punkty dostępowe podejmują próbę dostarczenia buforowanych ramek do uśpionych stacji. Praktycznym uzasadnieniem takiego rozwiązania jest fakt, że znacznie więcej energii wymaga uruchomienie nadajnika niż po prostu włączenie odbiornika. Projektanci standardu 802.11 przewidzieli powstanie zasilania bateryjnego stacji przenośnych. Rozwiązanie umożliwiające dostarczanie buforowanych ramek stacjom w pewnych odstępach czasu okazało się sposobem na przedłużenie żywotności baterii w urządzeniach o małej mocy.

Częścią operacji buforowania jest wysłanie do sieci elementu informacyjnego TIM (*Traffic Indication Map*), pokazanego na rysunku 4.36, i poinformowanie stacji, że posiadają do odebrania buforowany ruch.



Rysunek 4.36. Element informacyjny Traffic Indication Map

Jądrem elementu TIM jest *wirtualna bitmapa* (*virtual bitmap*), czyli logiczna struktura składająca się z 2 008 bitów. Każdy bit jest związany z Association ID. Kiedy ruch jest buforowany dla tego właśnie identyfikatora, bit ma wartość 1. Jeśli nie ma buforowanego ruchu, bit związany z AID wynosi 0.

Treść elementu informacyjnego TIM składa się z czterech części.

DTIM Count

To jednobajtowe pole jest liczbą ramek Beacon, które będą transmitowane przed kolejną ramką DTIM. Ramki DTIM informują, że wkrótce transmitowane będą

buforowane ramki typu broadcast i multicast. Nie wszystkie ramki Beacon są ramkami DTIM.

DTIM Period

To jednobajtowe pole podaje liczbę odstępów typu Beacon między ramkami DTIM. Zero jest zarezerwowane i nie używa się go. Licznik DTIM zmniejsza się wraz ze zwiększaniem się liczby cykli aż do zera.

Bitmap Control oraz *Partial Virtual Bitmap*

Pole Bitmap Control zostało podzielone na dwa podpola. Bit 0 jest używany dla wskaźnika ruchu identyfikatora AID 0, który jest zarezerwowany dla ruchu typu multicast. Pozostałe siedem bitów pola Bitmap Control są wykorzystane przez pole Bitmap Offset.

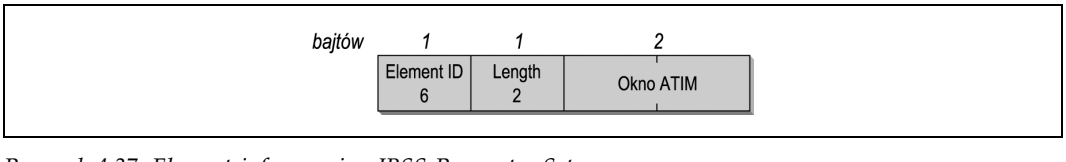
Dla zaoszczędzenia przepustowości pole Bitmap Offset może być wykorzystywane do transmisji części wirtualnej bitmapy. Bitmap Offset jest powiązany z początkiem bitmapy wirtualnej. Posługując się polami Bitmap Offset i Length, stacje przenośne mogą wydedukować, która część wirtualnej bitmapy została dołączona.

CF Parameter Set

Element informacyjny CF (Contention-Free) Parameter Set jest transmitowany w ramkach typu Beacon przez punkty dostępowe, które obsługują operację bez rywalizacji o dostęp. Usługa bez rywalizacji o dostęp do nośnika została omówiona w rozdziale 8., jest bowiem rozwiązaniem opcjonalnym.

IBSS Parameter Set

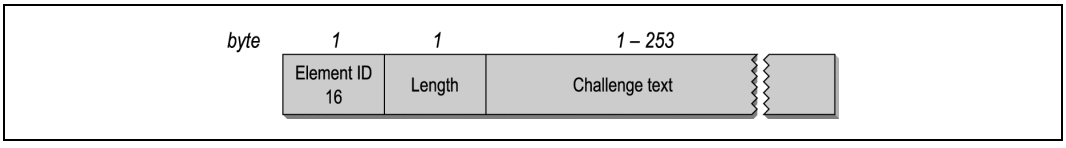
Sieci IBSS mają obecnie tylko jeden parametr — okno ATIM (*Announcement Traffic Indication Map*) pokazane na rysunku 4.37. Pole to jest wykorzystywane wyłącznie w ramkach Beacon w sieciach IBSS. Podaje ono liczbę jednostek czasu (TU) między ramkami ATIM w sieci IBSS.



Rysunek 4.37. Element informacyjny IBSS Parameter Set

Challenge Text

System uwierzytelniający typu Shared-Key zdefiniowany przez specyfikację 802.11 wymaga, by stacja przenośna potrafiła dekodować i kodować sygnał wezwania (*challenge*). Wezwanie to jest wysyłane za pomocą elementu informacyjnego Challenge Text, pokazanego na rysunku 4.38.



Rysunek 4.38. Element informacyjny Challenge Text

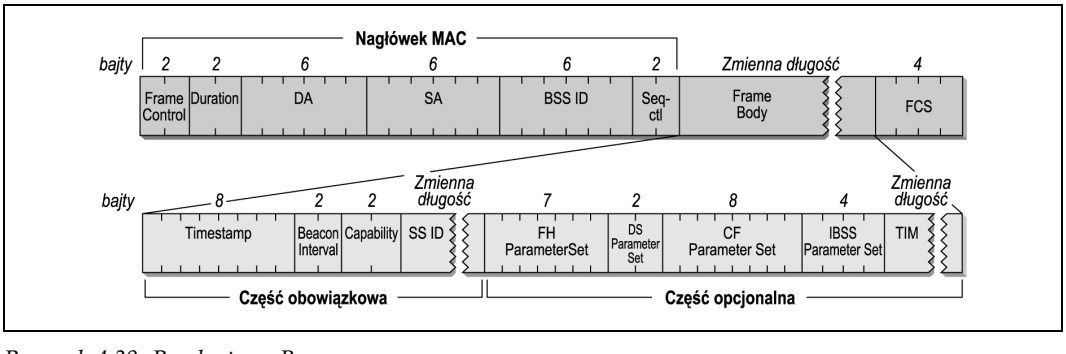
Typy ramek zarządzających

Aby pola stałe oraz elementy informacyjne mogły przenosić informacje, są umieszczane w treści ramek zarządzających. Istnieje kilka typów ramek zarządzających i są one stosowane do wielu różnorodnych funkcji utrzymania warstwy łącza danych.

Beacon

Ramki typu Beacon informują o istnieniu sieci i są ważną częścią wielu czynności utrzymujących sieć. Są one transmitowane w regularnych odstępach czasu, co umożliwia stacjom przenośnym znalezienie i zidentyfikowanie sieci, a także podłączenie się do niej dzięki dopasowaniu parametrów. W sieci stacjonarnej za transmitowanie ramek typu Beacon odpowiedzialny jest punkt dostępowy. Obszar, na jakim pojawiają się transmitowane przez niego ramki typu Beacon, stanowi zasięg BSS. Ponieważ cała komunikacja w sieci stacjonarnej odbywa się za pośrednictwem punktu dostępowego, wszystkie stacje, chcąc uczestniczyć w sieci, muszą znajdować się wystarczająco blisko niego, by „usłyszeć" ramki Beacon.

Rysunek 4.39 przedstawia wszystkie pola, które mogą być użyte w ramce Beacon w kolejności, w jakiej się tam pojawiają. Nie wszystkie te elementy są obecne w każdej ramce Beacon, co oznacza, że opcjonalne pola występują tam tylko, gdzie istnieje ku temu zasadniczy powód. FH i DS Parameter Set są wykorzystywane, tylko gdy podstawowa warstwa fizyczna opiera się na technikach rozpraszania skokowego lub sekwencyjnego. Tylko jedna warstwa fizyczna może być używana w danym momencie, więc FH i DS Parameter Set wzajemnie się wykluczają.



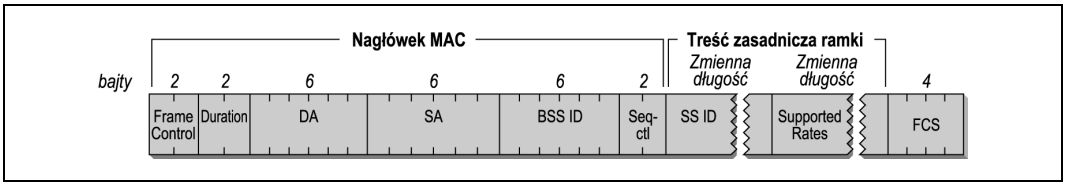
Rysunek 4.39. Ramka typu Beacon

CF Parameter Set jest stosowany jedynie w ramkach generowanych przez punkty dostępowe obsługujące PCF, co jest funkcją opcjonalną. Element TIM występuje tylko w ramkach

Beacon generowanych przez punkty dostępowe, ponieważ wyłącznie punkty dostępowe mogą wykonywać buforowanie ramek.

Probe Request

Stacje przenośne stosują ramki Probe Request do skanowania otoczenia w poszukiwaniu sieci bezprzewodowych. Format takiej ramki został przedstawiony na rysunku 4.40. Wszystkie pola ramki są obowiązkowe.



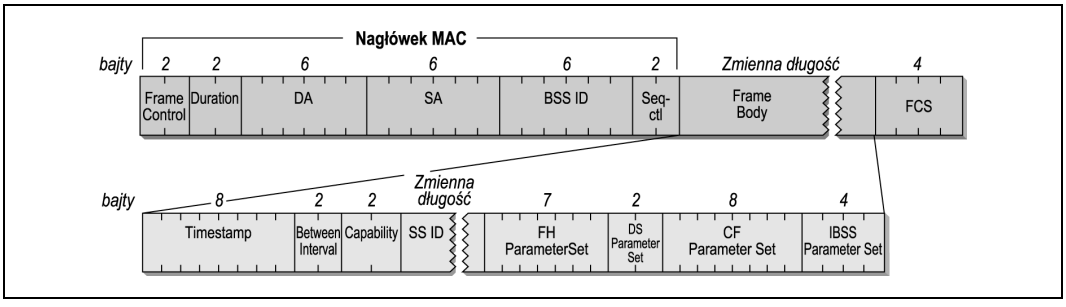
Rysunek 4.40. Ramka Probe Request

Ramka Probe Request zawiera dwa pola; SSID i szybkości transmisji obsługiwane przez daną stację przenośną (Supported Rates). Stacje otrzymujące ramki Probe Request posługują się tą informacją, by ocenić, czy dana stacja może przyłączyć się do sieci. Aby związek ten trwał długo i szczęśliwie, stacja przenośna musi obsługiwać wszystkie szybkości transmisji danych wymagane przez sieć oraz musi wyrazić wolę podłączenia się do sieci o danym SSID. Pole to może być ustawione na SSID konkretnej sieci lub w sposób umożliwiający podłączenie się do jakiejkolwiek kompatybilnej sieci. Sterowniki pozwalające kartom na przyłączenie się do dowolnej sieci stosują w ramkach Probe Request identyfikator SSID typu broadcast.

Probe Response

Jeśli ramka Probe Request napotka na sieć o kompatybilnych parametrach, otrzymuje od niej odpowiedź w postaci ramki Probe Response. Stacja, która wysyłała ostatnią ramkę Beacon jest odpowiedzialna za udzielenie odpowiedzi na wchodzące zapytania. W sieciach stacjonarnych stacją tą jest punkt dostępowy. W sieci IBSS odpowiedzialność za transmisję ramek Beacon jest rozłożona na stacje przenośne. Po wysłaniu ramki Beacon stacja taka ponosi odpowiedzialność za wysyłanie ramek Probe Response przez następny odstęp czasu typu Beacon. Format ramki Probe Response został przedstawiony na rysunku 4.41. Niektóre z jej pól wzajemnie się wykluczają; reguły obowiązujące dla ramek Beacon odnoszą się również do ramek Probe Response.

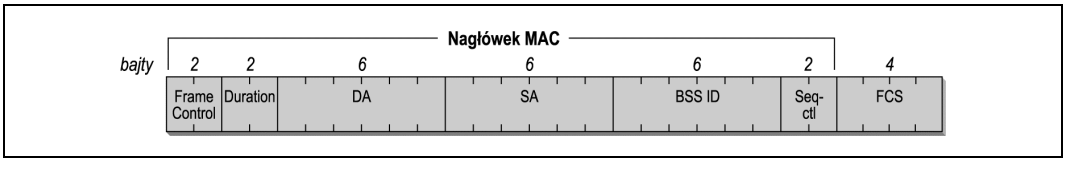
Ramka Probe Response wszystkie parametry przenosi w ramce Beacon, co pozwala stacjom przenośnym dopasować parametry i włączyć się do sieci. Ramki Probe Response mogą ze spokojem opuścić element TIM, ponieważ stacje wysyłające ramki typu Probe nie są jeszcze skojarzone z siecią i dlatego nie potrzebują wiedzy na temat, które skojarzenia mają do odebrania ramki buforowane przez punkt dostępowy.



Rysunek 4.41. Ramka Probe Response

ATIM w sieciach IBSS

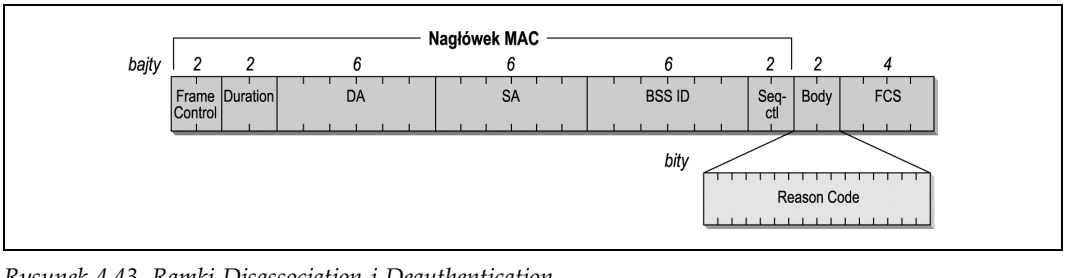
Sieci IBSS nie posiadają punktów dostępowych, a więc nie mogą od nich uzależniać funkcji buforowania danych. Kiedy stacja znajdująca się w sieci IBSS posiada buforowane ramki dla odbiornika w trybie oszczędnym, wysyła ramkę ATIM w okresie wysyłania danych w celu poinformowania odbiorcy o tym fakcie (patrz rysunek 4.42).



Rysunek 4.42. Ramka ATIM

Disassociation i Deauthentication

Ramki typu Disassociation (zerwanie skojarzenia) służą do kończenia relacji skojarzenia, a ramki typu Deauthentication (zerwanie uwierzytelnienia) służą do kończenia relacji uwierzytelnienia. Oba rodzaje ramek zawierają jedno stałe pole Reason Code, pokazane na rysunku 4.43. Oczywiście pola Frame Control różnią się, ponieważ to pole Subtype odróżnia od siebie typy ramek zarządzających.

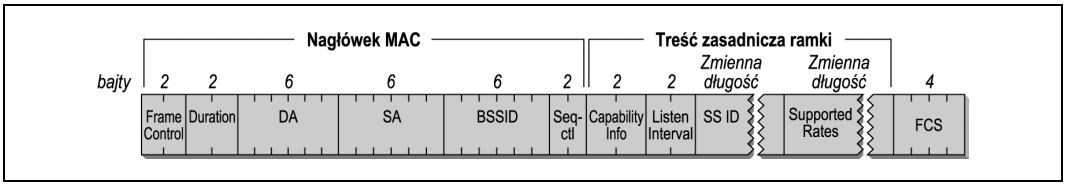


Rysunek 4.43. Ramki Disassociation i Deauthentication

Association Request

Kiedy stacja przenośna zidentyfikuje kompatybilną sieć i zostanie przez nią uwierzytelniona, może podjąć próbę podłączenia się do niej przez wysłanie ramki Association Request.

Format ramki Association Request został przedstawiony na rysunku 4.44. Wszystkie pola są obowiązkowe i muszą pojawiać się zawsze w kolejności pokazanej poniżej.

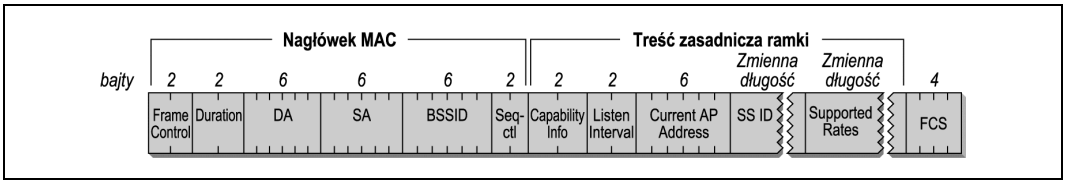


Rysunek 4.44. Ramka Association Request

Pole Capability Information służy do informowania o typie sieci, do jakiej stacja przenośna chciałaby się podłączyć. Zanim punkt dostępowy przyjmie zapytanie o skojarzenie, weryfikuje, czy Capability Information, SSID i Supported Rates pasują do wszystkich parametrów sieci. Punkty dostępowe zwracają uwagę również na Listen Interval, który precyzuje, jak często dana stacja słucha ramek Beacon podczas monitorowania TIM.

Reassociation Request

Stacje przenośne poruszające się między obszarami BSS w granicach tej samej sieci ESS są zmuszone do ponownego skojarzenia, zanim będą mogły posługiwać się znowu systemem dystrybucyjnym. Stacje mogą również wymagać ponownego skojarzenia, kiedy na jakiś czas wyjdą poza zasięg punktu dostępowego i chcą do niego powrócić (patrz rysunek 4.45).

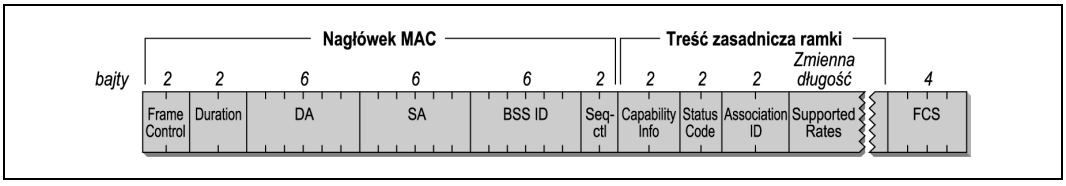


Rysunek 4.45. Ramka Reassociation Request

Ramki Association Request i Reassociation Request różnią się jedynie tym, że ta druga zawiera adres obecnego punktu dostępowego danej stacji przenośnej. Zamieszczenie tej informacji gwarantuje możliwość skontaktowania się nowego punktu ze starym punktem i przekazanie danych dotyczących operacji skojarzenia. Transfer ten może zawierać również ramki, które były buforowane przez stary punkt dostępowy.

Association Response i Reassociation Response

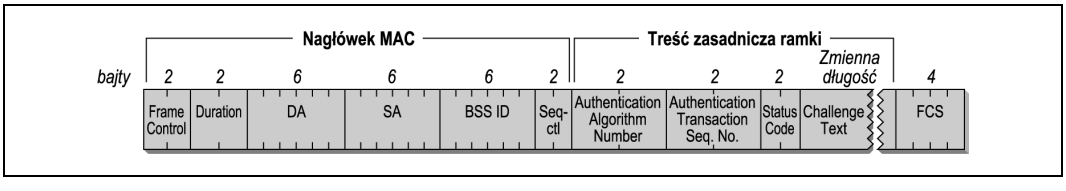
Kiedy stacje przenośne podejmują próbę skojarzenia z punktem dostępowym, otrzymują od niego odpowiedź w formie ramki Association Response lub Reassociation Response, pokazanej na rysunku 4.46. Oba typy ramek różnią się jedynie polem Subtype w polu Frame Control. Wszystkie pola są obowiązkowe. Jako element odpowiedzi punkt dostępowy przyznaje Association ID. Sposób, w jaki dokonuje tego przyznania, zależy od implementacji.



Rysunek 4.46. Ramka (Re)Association Response

Authentication

Aby otrzymać uwierzytelnienie, stacje przenośne wymieniają ramki Authentication, pokazane na rysunku 4.47.



Rysunek 4.47. Ramka Authentication

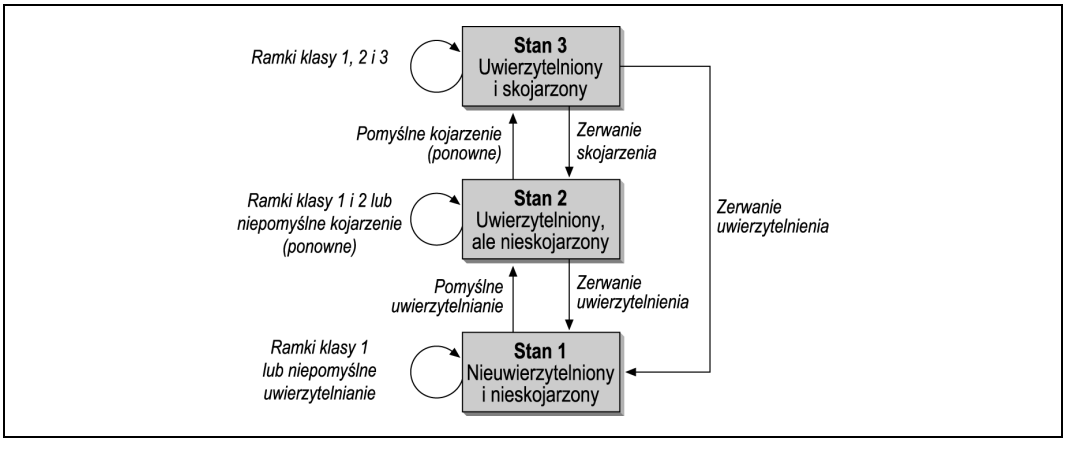
Różne rodzaje algorytmów uwierzytelniających mogą istnieć obok siebie. Do wybierania żądanego algorytmu służy pole Authentication Algorithm Number. Proces uwierzytelniania może wymagać kilku kroków (w zależności od algorytmu), a więc w procesie uwierzytelniania każda ramka otrzymuje swój numer w sekwencji. Pola Status Code i Challenge Text są inaczej wykorzystywane przez różne algorytmy; szczegóły tego zagadnienia znajdują się w rozdziale 7.

Transmisja ramek oraz stany skojarzenia i uwierzytelnienia

Dozwolone typy ramek różnią się pod względem stanów skojarzenia (powiązania) i uwierzytelnienia. Stacje otrzymują uwierzytelnienie albo go nie otrzymują i są skojarzone lub nie. Te dwie zmienne mogą w wyniku kombinacji dać trzy możliwe stany, stanowiące bezprzewodową hierarchię rozwoju sieci.

1. Stan początkowy; nieuwierzytelniony i nieskojarzony.
2. Uwierzytelniony, ale jeszcze nieskojarzony.
3. Uwierzytelniony i skojarzony.

Każdy stan jest sukcesywnie wyższym szczeblem rozwoju w połączeniach bezprzewodowych. Wszystkie stacje przenośne rozpoczynają od stanu 1., a dane mogą być transmitowane przez system dystrybucyjny znajdujący się jedynie w stanie 3. (Sieci IBSS nie mają punktów dostępowych ani związanych z nimi skojarzeń i dlatego osiągają tylko stan 2.). Rysunek 4.48 jest ogólnym diagramem stanów transmisji ramek w standardzie 802.11.



Rysunek 4.48. Ogólny diagram stanów w standardzie 802.11

Klasy ramek

Ramki zostały również podzielone na różne klasy. Ramki klasy 1. mogą być transmitowane w stanie 1.; ramki klasy 1. i 2. w stanie 2.; ramki klasy 1., 2. i 3. w stanie 3.

Ramki klasy 1

Ramki klasy 1. mogą być transmitowane w każdym stanie i są wykorzystywane do podstawowych operacji przeprowadzanych przez stacje bezprzewodowe. Ramki kontrolne są odbierane i przetwarzane, tak by możliwe było zachowanie podstawowych „reguł drogi" CSMA/CA oraz transmitowanie ramek w sieci IBSS. Ramki klasy 1. pomagają stacjom znaleźć sieć stacjonarną i uzyskać od niej uwierzytelnienie. Tabela 4.9 prezentuje listę ramek, które należą do klasy 1.

Tabela 4.9. Ramki klasy 1

Ramki kontrolne	Ramki zarządzające	Ramki danych
RTS (Request To Send)	Probe Request	Wszystkie ramki z ToDS i FromDS o wartości fałsz (0).
CTS (Clear To Send)	Probe Response	
ACK (Acknowledgement)	Beacon	
CF-End	Authentication	
CF-End+CF-Ack	Deauthentication	
	ATIM (Announcement Traffic Indication Message)	

Ramki klasy 2

Ramki klasy 2. mogą być transmitowane, tylko gdy stacja otrzyma uprzednio od sieci uwierzytelnienie, i mogą być używane jedynie w stanie 2. i 3. Ramki klasy 2. zarządzają

skojarzeniami. Pomyślne skojarzenie lub ponowne skojarzenie przesuwają ramkę do stanu 3.; niepomyślnie zakończone próby skojarzenia powodują, że ramka pozostaje w stanie 2. Kiedy stacja otrzymuje ramkę klasy 2. od nieuwierzytelnionej stacji, odpowiada ramką Deauthentication, przerzucając ją z powrotem do stanu 1[4]. Tabela 4.10 prezentuje listę ramek, które należą do klasy 2.

Tabela 4.10. Ramki klasy 2

Ramki kontrolne	Ramki zarządzające	Ramki danych
Brak	Association Request/Response Reassociation Request/Response Disassociation	Brak

Ramki klasy 3

Ramki klasy 3. są stosowane, gdy stacja została uwierzytelniona i skojarzona z punktem dostępowym. Kiedy stacja osiągnie stan 3., otrzymuje pozwolenie na korzystanie z usług systemu dystrybucyjnego i możliwość dotarcia do celów poza punktem dostępowym. Stacje mogą również korzystać z usług oszczędzania energii oferowanych przez punkt dostępowy w stanie 3. za pomocą ramki PS-Poll. Tabela 4.11 podaje typy ramek klasy 3.

Tabela 4.11. Ramki klasy 3

Ramki kontrolne	Ramki zarządzające	Ramki danych
PS-Poll	Deauthentication	Wszystkie ramki, w tym ramki z ustawionym bitem ToDS lub FromDS

Jeśli punkt dostępowy otrzymuje ramki od stacji przenośnej, która została uwierzytelniona, ale nie skojarzona, odpowiada on ramką Disassociation, żeby zawrócić stację do stanu 2. Jeśli stacja nie została nawet uwierzytelniona, punkt dostępowy odpowiada ramką Deauthentication, zmuszając stację do powrotu do stanu 1.

[4] Taka odmowa może mieć miejsce tylko w przypadku ramek, które nie zostały przefiltrowane. Filtrowanie zapobiega wywoływaniu odmowy.