

Projekt specyfikacji dla Projektu *Powerline Intelligent Metering Evolution*



Przygotowany przez PRIME Alliance Technical Working Group

Niniejszy dokument stanowi zatwierdzony projekt specyfikacji. W związku z tym może on ulec zmianie. Przed pełnym lub częściowym przyjęciem tego dokumentu przez organizację zajmującą się opracowywaniem norm, należy uzyskać zezwolenie od PRIME Alliance.

Streszczenie:

Jest to kompletny projekt specyfikacji dla nowej technologii komunikacji za pośrednictwem sieci zasilających opartej na OFDM mającej na celu świadczenie wszelkiego rodzaju usług inteligentnych systemów elektroenergetycznych (Smart Grid) w sieciach dystrybuujących energię elektryczną. W specyfikacji opisano obie warstwy PHY i MAC zgodnie z konwencjami IEEE oraz warstwę Konwergencji.

Spis treści

Spis treści	2
Wykaz rysunków	8
Wykaz tabel	12
1 Wstęp.....	18
1.1 Zakres.....	18
1.2 Omówienie	18
1.3 Odniesienia normatywne	18
1.4 Konwencje w dokumencie.....	20
1.5 Definicje.....	21
1.6 Skróty i akronimy	22
2 Opis ogólny	26
2.1 Wstęp.....	26
2.2 Opis ogólny architektury	26
3 Warstwa fizyczna.....	27
3.1 Wstęp.....	27
3.2 Omówienie	27
3.3 Parametry PHY.....	28
3.4 Struktura preambuły, nagłówka i treści	30
3.4.1 Preambuła	30
3.4.2 Struktura pilotowa.....	30
3.4.3 Nagłówek i treść	32
3.5 Koder splotowy.....	33
3.6 Scrambler.....	34
3.7 Urządzenie przeplatające	34
3.8 Modulacja	35
3.9 Parametry elektryczne nadajnika	37

3.9.1	Ogólne	37
3.9.2	PSD nadajnika	37
3.9.3	Wielkość wektora błędu (EVM)	39
3.9.4	Przeprowadzone ograniczenia zakłóceń.....	39
3.10	Specyfikacja usługi PHY	40
3.10.1	Ogólne	40
3.10.2	Prymitywy płaszczyzny danych PHY	40
3.10.3	Prymitywy płaszczyzny kontrolnej PHY	43
3.10.4	Prymitywy zarządzania PHY	50
4	Warstwa Mac.....	57
4.1	Omówienie	57
4.2	Adresowanie	58
4.2.1	Ogólne	58
4.2.2	Przykład konwersji adresu	59
4.2.3	Adresowanie broadcast i multicast	61
4.3	Opis funkcjonalny MAC	61
4.3.1	Uruchomienie węzła podstawowego	61
4.3.2	Uruchamianie i zarządzanie podsieciami	62
4.3.3	Dostęp do kanału	63
4.3.4	Śledzenie przełączeń i partnerzy	68
4.3.5	Przełączanie	69
4.3.6	Połączenia bezpośrednie	73
4.3.7	Agregacja pakietów	78
4.3.8	Zabezpieczenie	79
4.4	Format MAC PDU.....	84
4.4.1	Ogólne	84
4.4.2	Ogólna jednostka MAC PDU	84

4.4.3	Wymagana do promocji jednostka PDU	87
4.4.4	PDU sygnału	88
4.4.5	Pakiety kontrolne MAC	91
4.5	Punkt dostępu do usług MAC	113
4.5.1	Ogólne	113
4.5.2	Prymitywy sygnalizacji węzła serwisowego i węzła podstawowego	114
4.5.3	Prymitywy sygnalizacji węzła podstawowego	123
4.5.4	Prymitywy danych węzła podstawowego i węzła serwisowego	124
4.5.5	SAP jednostki zarządzającej warstwą MAC	125
4.6	Procedury MAC	133
4.6.1	Rejestracja	133
4.6.2	Proces wyrejestrowywania	135
4.6.3	Proces promocji	136
4.6.4	Proces degradacji	138
4.6.5	Proces utrzymania aktywności	139
4.6.6	Zarządzanie połączeniami	140
4.6.7	Zarządzanie grupą multicast	142
4.6.8	Zarządzanie odpornością warstwy PHY	147
4.6.9	Alokacja i dealokacji kanału	149
4.7	Automatyczne żądanie powtórzenia (ARQ)	150
4.7.1	Ogólne	150
4.7.2	Początkowe negocjowanie	150
4.7.3	Mechanizm ARQ	150
4.7.4	Przełączanie pakietów ARQ	154
5	Warstwa konwergencji	155
5.1	Omówienie	155
5.2	Podwarstwa styku CPCS	155

5.2.1	Ogólne	155
5.2.2	Podział i scalanie (SAR)	155
5.3	Zerowa podwarstwa konwergencji właściwa dla usługi (Zerowa SSCS).....	157
5.3.1	Omówienie	157
5.3.2	Prymitywy	157
5.4	IPv4 Podwarstwa konwergencji właściwa dla usługi (SSCS IPv4)	158
5.4.1	Omówienie	158
5.4.2	Konwersja adresu	160
5.4.3	Transfer pakietu IPv4.....	161
5.4.4	Podział i scalanie.....	162
5.4.5	Kompresja nagłówka	162
5.4.6	Mapowanie jakości usług	163
5.4.7	Formaty pakietów i dane połączenia.....	164
5.4.8	Punkt dostępu do usługi	169
5.5	IEC 61334-4-32 Podwarstwa konwergencji właściwa dla usługi (IEC 61334-4-32 SSCS).....	174
5.5.1	Ogólne	174
5.5.2	Omówienie	174
5.5.3	Alokacja adresu i nawiązywanie połączenia	175
5.5.4	Format danych ustanawiania połączenia	176
5.5.5	Format pakietu	177
5.5.6	Punkt dostępu do usługi	177
5.6	Podwarstwa konwergencji właściwa dla usługi IPv6 (SSCS IPv6)	179
5.6.1	Omówienie	179
5.6.2	Warstwa konwergencji IPv6	181
5.6.3	Konfiguracja adresu IPv6	182
5.6.4	Transfer pakietu IPv6.....	184
5.6.5	Podział i scalanie.....	185

5.6.6	Kompresja.....	185
5.6.7	Mapowanie jakości usług	185
5.6.8	Formaty pakietów i dane połączenia.....	186
5.6.9	Punkt dostępu do usługi	193
6	Płaszczyzna zarządzania.....	199
6.1	Wstęp.....	199
6.2	Zarządzanie węzłami.....	200
6.2.1	Ogólne	200
6.2.2	Atrybuty PIB warstwy PHY	200
6.2.3	Atrybuty PIB MAC	202
6.2.4	Atrybuty PIB aplikacji.....	216
6.3	Aktualizacja oprogramowania sprzętowego	216
6.3.1	Ogólne	216
6.3.2	Wymagania i funkcje	217
6.3.3	Opis ogólny	217
6.3.4	Atrybuty PIB oprogramowania sprzętowego	220
6.3.5	Mechanizm stanu	220
6.3.6	Przykłady.....	235
6.4	Opis interfejsu zarządzania.....	237
6.4.1	Ogólne	237
6.4.2	Format treści informacji zarządzania.....	238
6.4.3	Profil komunikacji zerowej warstwy SSCS	241
6.4.4	Profil komunikacji szeregowej	241
6.5	Lista obowiązkowych atrybutów PIB	242
6.5.1	Ogólne	242
6.5.2	Obowiązkowe atrybuty PIB wspólne dla wszystkich typów urządzeń.	242
6.5.3	Obowiązkowe atrybuty węzła podstawowego.....	243

6.5.4	Obowiązkowe atrybuty węzła serwisowego	243
	Załącznik A (informacyjny) Przykłady kontroli CRC	246
	Załącznik B (normatywny) Obliczenia EVM	247
	Załącznik C (informacyjny) Matryce przeplatania	248
	Załącznik D (normatywny) Stałe warstwy MAC.....	250
	Załącznik E (normatywny) Stałe warstwy konwergencji	251
	Załącznik F (normatywny) Profile	252
F.1	Profil pomiaru inteligentnego	252
	Załącznik G (informacyjny) Lista wykorzystanych częstotliwości	254
	Załącznik H (informacyjny) Informacyjny	256
H.1	Wymiana danych pomiędzy równorzędnymi IP	256
H.2	Dołączanie do grupy Multicast	258
	Załącznik I (informacyjny) Algorytm ARQ	260
	Lista autorów	261

Wykaz rysunków

Rys. 1 - Model referencyjny warstw protokołu stosowany w specyfikacji OFDM	26
Rys. 2 - Omówienie przetwarzania PPDU	28
Rys. 3 - Format ramki PHY	28
Rys. 4 - Alokacja podnośnej pilotowej i podnośnej danych (symbole OFDM w por. do podnośnych)	31
Rys. 5 - Alokacja częstotliwości podnośnej pilotowej i podnośnej danych wewnątrz nagłówka	31
Rys. 6 - LFSR do stosowania w generowaniu ciągu pilotowego	32
Rys. 7 - PPDU: nagłówek i treść (bity przesłane przed kodowaniem)	32
Rys. 8 - Koder splotowy	33
Rys. 9 - LFSR do stosowania w bloku scramblera	34
Rys. 10 - Mapowanie DBPSK, DQPSK i D8PSK.....	35
Rys. 11 - Mapowanie podnośnej	36
Rys. 12 – Konfiguracja pomiarów (jedna faza)	37
Rys. 13 – Konfiguracja pomiarów (trzy fazy)	38
Rys. 14 – Sieć sztuczna.....	38
Rys. 15 – Pomiar EVM (diagram blokowy)	39
Rys. 16 – Omówienie prymitywów PHY	40
Rys. 17 – Omówienie prymitywów płaszczyzny kontrolnej PHY	44
Rys. 18 - Stany węzła serwisowego	57
Rys. 19 - Struktura adresowania.....	59
Rys. 20 – Przykład konwersji adresu - faza 1	60
Rys. 21 – Przykład konwersji adresu - faza 2	60
Rys. 22 – Przykład konwersji adresu - faza 3	60
Rys. 23 – Przykład konwersji adresu - faza 4	61
Rys. 24 – Struktura ramki MAC.....	63
Rys. 25 – Przykład sekwencjonowania pakietu kontrolnego po promocji	65
Rys. 26 - Schemat dla algorytmu CSMA-CA.....	67

Rys. 27 - Przykład tablicy przełączania	70
Rys. 28 - Uzupełniona tablica przełączania.....	70
Rys. 29 – Połączenie przekierowane do nieznanego węzła serwisowego.....	74
Rys. 30 - Przykład połączenia bezpośredniego: ustanawianie połączenia ze znanym węzłem serwisowym..	76
Rys. 31 - Zwolnienie połączenia bezpośredniego.....	77
Rys. 32 - Koncept wyprowadzania klucza	81
Rys. 33 - Algorytm szyfrowania Profilu bezpieczeństwa 1	84
Rys. 34 - Ogólny format PDU MAC	84
Rys. 35 - Ogólny nagłówek MAC.....	84
Rys. 36 - Struktura pakietu	85
Rys. 37 – Nagłówek pakietu.....	86
Rys. 38 - Struktura PKT.CID.....	86
Rys. 39 - PDU MAC wymagana do promocji.....	87
Rys. 40 – Struktura PDU sygnału	89
Rys. 41 – Dwie transakcje niewymagające retransmisji	93
Rys. 42 - Transakcja ze stratą pakietów wymagająca retransmisji.....	94
Rys. 43 – Wykrywanie i eliminowanie duplikatów pakietów	94
Rys. 44 - Struktura pakietu kontrolnego REG	95
Rys. 45 - Struktura pakietu kontrolnego CON	99
Rys. 46 - Struktura pakietu kontrolnego PRO_REQ_S	102
Rys. 47 - Struktura pakietu kontrolnego PRO.....	102
Rys. 48 - Struktura pakietu kontrolnego BSI.....	105
Rys. 49 - Struktura pakietu kontrolnego FRA	106
Rys. 50 - Struktura pakietu kontrolnego CFP.....	106
Rys. 51 - Struktura pakietu kontrolnego ALV	108
Rys. 52 - Struktura pakietu kontrolnego MUL.....	109
Rys. 53 - Struktura pakietu kontrolnego PHY	110

Rys. 54 - Struktura pakietu kontrolnego SEC.....	112
Rys. 55 – Ustanawianie połączenia.....	113
Rys. 56 – Niepowodzenie ustanawiania połączenia	113
Rys. 57 – Zwolnienie połączenia	113
Rys. 58- Transfer danych	113
Rys. 59 – Zatwierdzony proces rejestracji	134
Rys. 60 – Odrzucony proces rejestracji.....	134
Rys. 61 – Proces wyrejestrowania inicjowany przez węzeł terminala	135
Rys. 62 – Proces wyrejestrowania inicjowany przez węzeł podstawowy	135
Rys. 63 – Proces promocji inicjowany przez węzeł serwisowy.....	137
Rys. 64 – Proces promocji odrzucony przez węzeł podstawowy	137
Rys. 65 – Proces promocji inicjowany przez węzeł podstawowy	138
Rys. 66 – Proces promocji odrzucony przez węzeł serwisowy	138
Rys. 67 – Proces degradacji inicjowany przez węzeł serwisowy	139
Rys. 68 – Proces degradacji inicjowany przez węzeł podstawowy.....	139
Rys. 69 – Ustanawianie połączenia inicjowane przez węzeł serwisowy	140
Rys. 70 – Ustanawianie połączenia odrzucone przez węzeł podstawowy	140
Rys. 71 – Ustanawianie połączenia inicjowane przez węzeł podstawowy.....	141
Rys. 72 – Ustanawianie połączenia odrzucone przez węzeł serwisowy.....	141
Rys. 73 – Rozłączanie inicjowane przez węzeł serwisowy.....	141
Rys. 74 – Rozłączanie inicjowane przez węzeł podstawowy	142
Rys. 75 – Udana dołączenie do grupy inicjowane przez węzeł podstawowy	143
Rys. 76 – Nieudane dołączenie do grupy inicjowane przez węzeł podstawowy	144
Rys. 77 – Udana dołączenie do grupy inicjowane przez węzeł serwisowy	145
Rys. 78 – Nieudane dołączenie do grupy inicjowane przez węzeł serwisowy.....	146
Rys. 79 – Opuszczenie grupy inicjowane przez węzeł serwisowy	147
Rys. 80 – Opuszczenie grupy inicjowane przez węzeł serwisowy	147

Rys. 81 – Zarządzanie odpornością warstwy PHY wnioskowane przez węzeł przełączający	148
Rys. 82 – Zarządzanie odpornością warstwy PHY wnioskowane przez węzeł serwisowy.....	148
Rys. 83 – Skuteczna alokacja okresu CFP.....	149
Rys. 84 – Sekwencja skutecznej dealokacji kanału	149
Rys. 85 – Dealokacja kanału do jednego urządzenia prowadzi do zmiany okresu CDP przydzielonego do innego urządzenia	150
Rys. 86 - PDU danych warstwy MAC z podnagłówkiem ARQ	151
Rys. 87 - Podnagłówek ARQ jedynie z identyfikatorem pakietu	151
Rys. 88 - Podnagłówek ARQ z ARQ.INFO	151
Rys. 89 - Pola bajta ARQ.ACK	151
Rys. 90 - Pola bajta ARQ.WIN	151
Rys. 91 - Pola bajtów ARQ.NACK	151
Rys. 92 - Przykład podnagłówka ARQ z wszystkimi polami	152
Rys. 93 - Podnagłówek ARQ Stop-and-Wait jedynie z identyfikatorem pakietu	153
Rys. 94 - Podnagłówek ARQ Stop-and-Wait z zatwierdzeniem (ACK)	153
Rys. 95 - Podnagłówek ARQ Stop-and-Wait bez danych i z ACK	154
Rys. 96 – Struktura warstwy konwergencji	155
Rys. 97 - Nagłówki podziału i scalania	156
Rys. 98 - Przykład połączenia podwarstwy SSCS IPv4.....	159
Rys. 99 – Przykład połączenia IPv6	181
Rys. 100 - Płaszczyzna zarządzania. Wprowadzenie.....	199
Rys. 101 - Ponowne uruchamianie węzłów z nowym oprogramowaniem sprzętowym.....	219
Rys. 102 - Mechanizm aktualizacji oprogramowania sprzętowego, diagram stanu	224
Rys. 103 - Inicjalizacja Węzła serwisowego i pełny obraz oprogramowania sprzętowego	235
Rys. 104 - Przeprowadzanie aktualizacji i zatwierdzenie/odrzuć nowej wersji oprogramowania.....	236
Rys. 105. Uzyskiwanie (GET) odpowiedzi atrybutu PIB. Treść.....	239
Rys. 106 – Hermetyzacja danych dla komunikatów zarządzania	241

Wykaz tabel

Tabela 1 parametry częstotliwości i czasu w warstwie PHY OFDM PRIME	28
Tabela 2 - parametry prędkości transmisji PHY oraz wielkości pakietów dla różnych modulacji i schematów kodowania	29
Tabela 3 - Parametry nagłówka	29
Tabela 4 - Pola skojarzone z prymitywami płaszczyzny kontrolnej warstwy PHY	44
Tabela 5 - Prymitywy zarządzania warstwą fizyczną	50
Tabela 6 – Wartości parametru statusu w prymitywie PLME_GET.confirm	55
Tabela 7 - Adres broadcast i multicast	61
Tabela 8 - Przykład połączenia bezpośredniego: Tablica przełączania bezpośredniego węzła B.....	75
Tabela 9 - Pola ogólnego nagłówka MAC	85
Tabela 10 – Pola nagłówka pakietu	86
Tabela 11 - PDU MAC wymagana do promocji.....	88
Tabela 12 - Pola PDU sygnału	89
Tabela 13 - Typy pakietu kontrolnego MAC	92
Tabela 14 - Pola pakietu kontrolnego REG	96
Tabela 15 - Typy pakietu kontrolnego REG	98
Tabela 16 - Pola pakietu kontrolnego CON	99
Tabela 17 - Typy pakietu kontrolnego CON.....	101
Tabela 18 - Pola pakietu kontrolnego PRO.....	102
Tabela 19 - Typy pakietu kontrolnego PRO	104
Tabela 20 - Pola pakietu kontrolnego BSI.....	105
Tabela 21 - Typy komunikatu kontrolnego BSI.....	105
Tabela 22 - Pola pakietu kontrolnego FRA	106
Tabela 23 - Typy pakietu kontrolnego FRA.....	106
Tabela 24 - Pola komunikatu kontrolnego CFP	107
Tabela 25 - Typy pakietu kontrolnego CFP	107

Tabela 26 - Pola komunikatu kontrolnego ALV	108
Tabela 27 - Typy pakietu kontrolnego Utrzymywania aktywności.....	108
Tabela 28 - Pola komunikatu kontrolnego MUL.....	109
Tabela 29 - Typy komunikatu kontrolnego MUL	110
Tabela 30 - Pola komunikatu kontrolnego PRM.....	110
Tabela 31 - Typy komunikatu kontrolnego PRM	111
Tabela 32 - Pola komunikatu kontrolnego SEC.....	112
Tabela 33 – Lista prymitywów MAC	113
Tabela 34 – Wartości parametru odpowiedzi <i>Answer</i> w prymitywie MAC_ESTABLISH.response.....	116
Tabela 35 – Wartości parametru wyniku <i>Result</i> w prymitywie MAC_ESTABLISH.confirm	117
Tabela 36 – Wartości parametru powodu <i>Reason</i> w prymitywie MAC_RELEASE.indication	118
Tabela 37 – Wartości parametru odpowiedzi <i>Answer</i> w prymitywie MAC_RELEASE.response	118
Tabela 38 – Wartości parametru wyniku <i>Result</i> w prymitywie MAC_RELEASE.confirm.....	119
Tabela 39 – Wartości parametru wyniku <i>Result</i> w prymitywie MAC_JOIN.confirm	121
Tabela 40 – Wartości parametru odpowiedzi <i>Answer</i> w prymitywie MAC_ESTABLISH.response.....	122
Tabela 41 – Wartości parametru wyniku <i>Result</i> w prymitywie MAC_LEAVE.confirm	123
Tabela 42 – Wartości parametru wyniku <i>Result</i> w prymitywie MAC_DATA.confirm	125
Tabela 43 – Wartości parametru wyniku <i>Result</i> w prymitywie MLME_REGISTER.confirm	126
Tabela 44 – Wartości parametru wyniku <i>Result</i> w prymitywie MLME_UNREGISTER.confirm	127
Tabela 45 – Wartości parametru wyniku <i>Result</i> w prymitywie MLME_PROMOTE.confirm	129
Tabela 46 – Wartości parametru wyniku <i>Result</i> w prymitywie MLME_DEMOTE.confirm	129
Tabela 47 – Wartości parametru wyniku <i>Result</i> w prymitywie MLME_RESET.confirm	130
Tabela 48 – Wartości parametru statusu w prymitywie MLME_GET.confirm	131
Tabela 49 – Wartości parametru statusu w prymitywie MLME_LIST_GET.confirm	132
Tabela 50 – Wartości parametru wyniku <i>Result</i> w prymitywie MLME_SET.confirm	133
Tabela 51 - Pola ARQ	152
Tabela 52 - Pola nagłówka SAR.....	156

Tabela 53 - Stałe SAR	157
Tabela 54 - Mapowanie prymitywów pomiędzy prymitywami podwarstwy zerowej SSCS a prymitywami warstwy MAC.....	158
Tabela 55 - Pozycja tablicy SSCS IPv4	161
Tabela 56 - Mapowanie pierwszeństwa IPv4 na priorytet MAC OFDM PRIME.....	163
Tabela 57 - Format komunikatu AR_REGISTER_S.....	164
Tabela 58 - Format komunikatu AR_REGISTER_B	164
Tabela 59 - format komunikatu AR_UNREGISTER_S	165
Tabela 60 - format komunikatu AR_UNREGISTER_B.....	165
Tabela 61 - format komunikatu AR_LOOKUP_S	165
Tabela 62 - format komunikatu AR_LOOKUP_B.....	166
Tabela 63 - format komunikatu AR_MCAST_REG_S	166
Tabela 64 - format komunikatu AR_MCAST_REG_B	166
Tabela 65 - format komunikatu AR_MCAST_UNREG_S	167
Tabela 66 - format komunikatu AR_MCAST_UNREG_B	167
Tabela 67 - Format pakietu IPv4 bez wynegocjowanej kompresji nagłówek.....	168
Tabela 68 - Format pakietu IPv4 z wynegocjowaną kompresją nagłówek.....	168
Tabela 69 - Dane sygnalizacji połączenia wysyłane przez inicjatora	169
Tabela 70 69 - Dane sygnalizacji połączenia wysyłane przez respondenta.....	169
Tabela 71 - Dane sygnalizacji połączenia wysyłane przez węzeł serwisowy	176
Tabela 72 - Dane sygnalizacji połączenia wysyłane przez węzeł podstawowy	177
Tabela 73 – Pozycje tablicy warstwy konwergencji IPv6.....	184
Tabela 74 – Mapowanie pierwszeństwa IPv6 na priorytet MAC PRIME	185
Tabela 75 - Format komunikatu AR_REGISTERv6_S.....	186
Tabela 76 - Format komunikatu AR_REGISTERv6_B	187
Tabela 77 - format komunikatu AR_UNREGISTERv6_S	187
Tabela 78 - format komunikatu AR_UNREGISTERv6_B.....	188
Tabela 79 - format komunikatu AR_LOOKUPv6_S	188

Tabela 80 - format komunikatu AR_LOOKUPv6_B	188
Tabela 81 - format komunikatu AR_MCAST_REGv6_S.....	189
Tabela 82 - format komunikatu AR_MCAST_REGv6_B	189
Tabela 83 - format komunikatu AR_MCAST_UNREGv6_S.....	190
Tabela 84 - format komunikatu AR_MCAST_UNREGv6_B	190
Tabela 85 - Format pakietu IPv6 bez wynegocjowanej kompresji nagłówków.....	191
Tabela 86 - Format pakietu UDP/IPv6 z kompresją nagłówków LOWPAN_IPHC1 i LOWPAN_NHC	191
Tabela 87 - Format pakietu IPv6 z wynegocjowaną kompresją nagłówków LOWPAN_IPHC	191
Tabela 88 - Dane sygnalizacji połączenia IPv6 wysyłane przez inicjatora	192
Tabela 89 - Dane sygnalizacji połączenia IPv6 wysyłane przez respondenta	193
Tabela 90 - Zmienne tylko do odczytu warstwy PHY dostarczające informacje statystyczne	200
Tabela 91 - Parametry tylko do odczytu warstwy PHY dostarczające informacje na temat określonego wdrożenia	202
Tabela 92 - Tablica zmiennych do odczytu/zapisu warstwy MAC.....	203
Tabela 93 - Tablica zmiennych tylko do odczytu warstwy MAC.....	205
Tabela 94 - Tablica zmiennych tylko do odczytu warstwy MAC, które dostarczają informacje funkcjonalne	205
Tabela 95 - Tablica zmiennych tylko do odczytu warstwy MAC, które dostarczają informacje statystyczne	209
Tabela 96 - Tablica listy tylko do odczytu udostępnianych przez warstwę MAC przez interfejs zarządzania	209
Tabela 97 - Atrybuty PIB działania	215
Tabela 98 - Atrybuty PIB aplikacji	216
Tabela 99 - Atrybuty PIB oprogramowania sprzętowego.....	220
Tabela 100 - Mechanizm stanu oprogramowania sprzętowego	220
Tabela 101 - Pola FU_INIT_REQ.....	225
Tabela 102 - Pola FU_EXEC_REQ	226
Tabela 103 - Pola FU_CONFIRM_REQ	227
Tabela 104 - Pola FU_STATE_REQ	227
Tabela 105 - Pola FU_KILL_REQ.....	228

Tabela 106 - Pola FU_STATE_RSP	228
Tabela 107 - Pola FU_DATA	229
Tabela 108 - Pola FU_MISS_REQ	230
Tabela 109 - Pola FU_MISS_BITMAP	230
Tabela 110 - Pola FU_MISS_LIST	231
Tabela 111 - Pola FU_INFO_REQ	231
Tabela 112 - Wartości dodatnie Infold	232
Tabela 113 - Pola FU_INFO_RSP	232
Tabela 114 - Pola każdej pozycji InfoData w FU_INFO_RSP	233
Tabela 115 - Pola FU_CRC_REQ	233
Tabela 116 - Pola FU_CRC_RSP	234
Tabela 117 - Zarządzanie danymi z pól	237
Tabela 118 - Pola żądania atrybutu PIB GET	238
Tabela 119 - Pola odpowiedzi atrybutu PIB GET	239
Tabela 120 - wspólne obowiązkowe atrybuty warstwy fizycznej PHY	242
Tabela 121 - Wspólne atrybuty obowiązkowe PIB MAC	242
Tabela 122 - Wspólne atrybuty obowiązkowe PIB aplikacji	243
Tabela 123 - Atrybuty obowiązkowe węzła podstawowego PIB MAC	243
Tabela 124 - Atrybuty obowiązkowe węzła serwisowego PIB MAC	244
Tabela 125 - Atrybuty obowiązkowe węzła serwisowego APP PIB	245
Tabela 126 – Przykłady CRC obliczonej dla różnych ciągów ASCII	246
Tabela 127 - Matryca przeplatania nagłówka.	248
Tabela 128 - Matryca przeplatania DBPSK(FEC WŁ.)	248
Tabela 129 - Matryca przeplatania DQPSK(FEC WŁ.)	248
Tabela 130 - Matryca przeplatania D8PSK(FEC WŁ.)	249
Tabela 131 - Tabela stałych MAC	250
Tabela 132 - Przydziały wartości TYPE	251

Tabela 133 - Przydziały wartości LCID	251
Tabela 134 - Wartości wynikowe dla prymitywów warstwy konwergencji	251
Tabela 135 – Lista wykorzystanych częstotliwości	254

1 Wstęp

Niniejszy dokument stanowi specyfikację techniczną technologii OFDM PRIME.

1.1 Zakres

Niniejszy dokument opisuje warstwę fizyczną PHY, warstwę MAC oraz warstwę Konwergencji dla efektywnej pod kątem złożoności, wąskopasmowej (< 20 kb/s) transmisji danych w liniach energetycznych, które mogą wchodzić w skład inteligentnego systemu elektroenergetycznego.

1.2 Omówienie

Celem niniejszego dokumentu jest określenie systemu wąskopasmowej transmisji danych opartego na schemacie modulacji OFDM mającego na celu świadczenie głównie usług połączeniowych.

Specyfikacja aktualnie opisuje:

- Warstwę fizyczną PHY mogącą osiągnąć przepływowość danych niekodowanych rzędu 128 kb/s (patrz rozdział 3).
- Warstwę MAC dla środowiska linii energetycznych (patrz rozdział 4).
- Warstwę Konwergencji do adaptacji kilku określonych usług (patrz rozdział 5).
- Płaszczyznę zarządzania (patrz rozdział 6)

Specyfikację napisano z perspektywy nadajnika celem zapewnienia współpracy pomiędzy urządzeniami i umożliwienia różnych implementacji.

1.3 Odniesienia normatywne

Poniższe publikacje zawierają postanowienia, które poprzez odniesienia do nich w niniejszym tekście, stanowią postanowienia niniejszej specyfikacji. W momencie publikacji wskazane edycje były aktualne. Wszystkie normy podlegają nowelizacji, a strony umowy, na podstawie niniejszej specyfikacji zachęcane są do sprawdzenia możliwości zastosowania najnowszego wydania następujących norm:

Lp.	Nr Ref.	Tytuł
[1]	EN 50065-1:2001+A1:2010	Transmisja sygnałów w sieciach elektrycznych niskiego napięcia w zakresie częstotliwości od 3 kHz do 148,5 kHz - Część 1: Ogólne wymagania, zakresy częstotliwości i zaburzenia elektromagnetyczne.
[2]	EN IEC 50065-7:2001	PN-EN 50065-7:2002 Transmisja sygnałów w sieciach elektrycznych niskiego napięcia w zakresie częstotliwości od 3 kHz do 148,5 kHz - Część 7: Impedancja sprzętu.

Lp.	Nr Ref.	Tytuł
[3]	IEC 61334-4-1:1996	Automatyzacja sieci rozdzielczej z użyciem łączności wykorzystującej tę sieć - Część 4-1: Protokoły transmisji danych. Model odniesienia systemu komunikacyjnego.
[4]	IEC 61334-4-32:1996	Automatyzacja sieci rozdzielczej z użyciem łączności wykorzystującej tę sieć - Część 4-32: Protokoły transmisji danych. Warstwa łącza danych. Sterowanie łączem logicznym (LLC).
[5]	IEC 61334-4-511:2000	Automatyzacja sieci rozdzielczej z użyciem łączności wykorzystującej tę sieć - Część 4-511: Protokoły transmisji danych. Zarządzanie systemami. Protokół CIASE.
[6]	IEC 61334-4-512:2001	Automatyzacja sieci rozdzielczej z użyciem łączności wykorzystującej tę sieć - Część 4-512: Protokoły transmisji danych. Zarządzanie systemami z użyciem profilu 61334-5-1. Zarządzanie.
[7]	prEN/TS 52056-8-4	Wymiana danych w pomiarach energii elektrycznej - Zespół DLMS/COSEM - Część 8-4: Profil typu 1 modulacji Ortogonalnego zwielokrotniania w dziedzinie częstotliwości (OFDM).
[8]	Standard IEEE 802.2001	Standard IEEE w sprawie sieci lokalnych i miejskich. Omówienie i architektura.
[9]	IETF RFC 768	Protokół pakietów użytkownika (UDP) [online]. Pod redakcją J. Postel. Sierpień 1980. Dostępny na: https://www.ietf.org/rfc/rfc768.txt
[10]	IETF RFC 791	Protokół internetowy (IP) [online]. Redakcja: Instytut Informatyki, Uniwersytet Południowej Karoliny. Wrzesień 1981. Dostępny na: https://www.ietf.org/rfc/rfc791.txt
[11]	IETF RFC 793	Protokół kontroli transmisji (TCP) [online]. Redakcja: Instytut Informatyki, Uniwersytet Południowej Karoliny. Wrzesień 1981. Dostępny na: https://www.ietf.org/rfc/rfc793.txt
[12]	IETF RFC 1144	Kompresja nagłówek TCP/IP dla łączy szeregowych o niskiej prędkości [online]. Pod redakcją V. Jacobsona. Luty 1990. Dostępny na: https://www.ietf.org/rfc/rfc1144.txt
[13]	IETF RFC 2131	Protokół dynamicznego konfigurowania węzłów (DHCP) [online]. Pod redakcją R. Droms. Marzec 1997. Dostępny na: https://www.ietf.org/rfc/rfc2131.txt

Lp.	Nr Ref.	Tytuł
[14]	IETF RFC 2460	Protokół internetowy, Wersja 6 (IPv6), Specyfikacja [online]. Pod redakcją S. Deering, R. Hinden. Grudzień 1998. Dostępny na: https://www.ietf.org/rfc/rfc2460.txt
[15]	IETF RFC 3022	Tradycyjny Translator Adresów Sieciowych IP (NAT) [online] Pod redakcją P. Srisuresh, Jasmine Networks, K. Egevang. Styczeń 2001. Dostępny na: https://www.ietf.org/rfc/rfc3022.txt
[16]	NIST FIPS-197	Specyfikacja dla ZAAWANSOWANEGO STANDARDU SZYFROWANIA (AES), http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf
[17]	NIST SP 800-57	Zalecenie dotyczące zarządzania kluczami. Część 1: Ogólna (Poprawiona). Dostępny na http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf
[18]	NIST SP800-38A:2001	Zalecenia dla trybów pracy szyfrów blokowych. Metody i techniki. Dostępny na http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf
[19]	IETF RFC 4191	IP wersja 6. Architektura adresowania Dostępny na http://tools.ietf.org/html/rfc4291
[20]	IETF RFC 6282	IP wersja 6. Datagramy na IEEE 802.15.4. Dostępny na http://tools.ietf.org/html/rfc6282
[21]	IETF RFC 4862	Bezstanowa konfiguracja adresu. Dostępny na http://www.ietf.org/rfc/rfc4862.txt
[22]	IETF RFC 2464	Przesyłanie pakietów IPv6 przez sieci Ethernet. Dostępny na http://www.ietf.org/rfc/rfc4862.txt

1.4 Konwencje w dokumencie

Niniejszy dokument został podzielony na rozdziały i załączniki. Treści dokumentu (wszystkie rozdziały) ma charakter normatywny (z wyjątkiem tekstów podanych kursywą). Załączniki mogą być normatywne lub informacyjne według wskazania dla każdego załącznika.

Liczby binarne są oznaczone prefiksem „0b”, po którym następują cyfry binarne, np. „0b0101”. Liczby szesnastkowe są oznaczone prefiksem „0x”.

Wymagania obowiązkowe są oznaczone słowem „należy” w treści niniejszego dokumentu.

Wymagania opcjonalne są oznaczone słowem „można” w treści niniejszego dokumentu. Jeśli opcja jest włączona w realizację, będzie ona stosowana w sposób określony w tym dokumencie.

- 33 roof (.) oznacza zaokrąglenie do najbliższej wyższej lub równej liczby całkowitej.
- 34 floor (.) oznacza zaokrąglenie do najbliższej niższej lub równej liczby całkowitej.
- 35 $A \bmod B$ oznacza resztę (z 0, 1, ..., B-1) uzyskaną, gdy liczba całkowita A dzieli się przez liczbę całkowitą B.

36 1.5 Definicje

37

Termin	Opis
Węzeł podstawowy	Węzeł główny, który kontroluje i zarządza zasobami podsieci.
Szczelina sygnału	Lokalizacja PDU sygnału w ramce.
Węzeł docelowy	Węzeł otrzymujący ramkę.
Połączenie pobierające (Downlink)	Dane przechodzące w kierunku od węzła podstawowego do węzła serwisowego
Poziom (Warstwa PHY)	Gdy termin stosowany jest w kontekście warstwy fizycznej (PHY), oznacza poziom mocy przesyłania.
Poziom (Warstwa MAC)	Gdy termin stosowany jest w kontekście zarządzania dostępem do medium (MAC), oznacza położenie urządzenia referencyjnego w hierarchii przełączania.
Ramka MAC	Kompozytowa jednostka abstrakcji czasu do stosowania w kanałach. Ramka MAC składa się z jednego lub więcej sygnałów (Beacon), jednego okresu SCP i zero lub jednego okresu CFP. Przesyłanie sygnału przez węzeł podstawowy działa jako ogranicznik dla ramki MAC.
Węzeł sąsiadujący	Węzeł A jest Węzłem sąsiadującym Węzła B jeśli A może bezpośrednio przesyłać dane do i odbierać od B.
Węzeł	Dowolny element podsieci potrafiący przesyłać i odbierać dane od innych elementów podsieci.
Ramka PHY	Zestaw symboli OFDM i preambuły, który stanowi pojedynczą jednostkę PPDU
Preambuła	Początkowa część ramki PHY, używana do synchronizacji celów
Rejestracja	Proces, w którym Węzeł serwisowy zatwierdzany jest jako członek podsieci i przydzielany jest mu LNID.
Węzeł serwisowy	Dowolny węzeł podsieci, który nie jest węzłem podstawowym.
Węzeł źródłowy	Węzeł wysyłający ramkę.

Termin	Opis
Podsieć	Zestaw elementów, które mogą się komunikować zgodnie z niniejszą specyfikacją i współdzielić pojedynczy węzeł podstawowy.
Adres podsieci	Właściwość, która uniwersalnie identyfikuje podsieć. Jest to adres EUI-48 węzła podstawowego.
Przełączanie	Zapewnienie łączności pomiędzy węzłami, które nie są węzłami sąsiadującymi.
Wyrejestrowanie	Proces, w którym Węzeł serwisowy opuszcza podsieć.
Łącze ładowania (Uplink)	Dane przechodzące w kierunku od węzła serwisowego do węzła podstawnego

38

39 1.6 Skróty i akronimy

Termin	Opis
AC	Prąd przemienny
AES	Zaawansowany standard szyfrowania
AMM	Zaawansowane zarządzanie pomiarami
ARQ	Automatyczne żądanie powtórzenia
ATM	Tryb transferu asynchronicznego
BER	Współczynnik błędnych bitów
BPDU	PDU sygnału
BPSK	Binarne kluczkowanie z przesunięciem fazy
CENELEC	Europejski Komitet Normalizacyjny Elektrotechniki
CFP	Okres bezkolizyjnego dostępu
CID	Identyfikator połączenia
CL	Warstwa konwergencji
CIMTUSize	Maksymalny rozmiar jednostki transmisyjnej warstwy konwergencji
CPCS	Podwarstwa styku CPCS
CRC	Cykliczna kontrola nadmiarowa

Termin	Opis
CSMA-CA	Protokół jednoczesnego dostępu z wykrywaniem i unikaniem kolizji
D8PSK	Różnicowe ośmiopoziomowe kluczowanie z przesunięciem fazy
DBPSK	Binarne kluczowanie z przesunięciem fazy
DHCP	Protokół dynamicznego konfigurowania węzłów
DPSK	Różnicowe kluczowanie z przesunięciem fazy (ogólne)
DQPSK	Różnicowe czteropoziomowe kluczowanie z przesunięciem fazy
DSK	Klucz tajny urządzenia
ECB	Elektroniczna książka kodowa
EMA	Wykładnicza średnia krocząca
ENOB	Efektywna liczba bitów
EUI-48	48-bitowy rozszerzony unikalny identyfikator
EVM	Wielkość wektora błędu
FCS	Sekwencja kontrolna ramki
FEC	Korekcja FEC
FFT	Szybkie przekształcenie Fouriera
GK	Klucz generowania
GPDU	Ogólna jednostka MAC PDU
HCS	Suma kontrola nagłówka
IEC	Międzynarodowa Komisja Elektrotechniczna
IEEE	Instytut Inżynierów Elektryków i Elektroników
IFFT	Odwrotne szybkie przekształcenie Fouriera
IGMP	Protokół zarządzania grupami internetowymi
IPv4	Protokół internetowy, wersja 4
kb/s	kilobity na sekundę
KDIV	Dywersyfikator kluczy

Termin	Opis
LCID	Identyfikator połączenia lokalnego
LFSR	Rejestr przesuwany z liniowym sprzężeniem zwrotnym
LLC	Sterowanie połączeniem logicznym
LNID	Identyfikator węzła lokalnego
LSID	Identyfikator przełączenia lokalnego
LWK	Lokalny klucz roboczy
MAC	Kontrola dostępu do medium
MK	Klucz główny
MLME	Jednostka zarządzająca warstwą MAC
MPDU	Jednostka danych protokołu MAC
nzb	Najbardziej znaczący bit
MSDU	Jednostka danych usługi MAC
MSPS	Miliony próbek na sekundę
MTU	Maksymalna jednostka transmisyjna
NAT	Tłumaczenie adresów sieciowych
NID	Identyfikator węzła
NSK	Klucz tajny sieci
OFDM	Ortogonalne zwielokrotnianie w dziedzinie częstotliwości
PDU	Jednostka danych protokołu
PHY	Warstwa fizyczna
PIB	Baza informacji PLC
PLC	Komunikacja PLC
PLME	Jednostka zarządzająca warstwą fizyczną
PNPDU	Wymagana do promocji jednostka PDU
PPDU	Jednostka danych protokołu PHY

Termin	Opis
ppm	Części na milion
PSD	Gęstość widmowa mocy
PSDU	Jednostka danych usługi PHY
QoS	Jakość usługi
SAP	Punkt dostępu do usługi
SAR	Podział i scalanie
SCP	Okres współdzielonej kontencji
SCRC	Kontrola CRC zabezpieczeń
SDU	Jednostka danych usługi
SEC	Zabezpieczenie
SID	Identyfikator przełączenia
SNA	Adres podsieci
SNK	Klucz podsieci (odpowiada REG.SNK lub SEC.SNK)
SNR	Stosunek sygnału do szumu
SP	Profil zabezpieczeń
SSCS	Podwarstwa konwergencji właściwa dla usługi
SWK	Klucz roboczy podsieci
TCP	Protokół kontroli transmisji
TOS	Typ usługi
UI	Unikalny identyfikator
USK	Unikalny tajny klucz
VJ	Van Jacobson
WK	Klucz roboczy

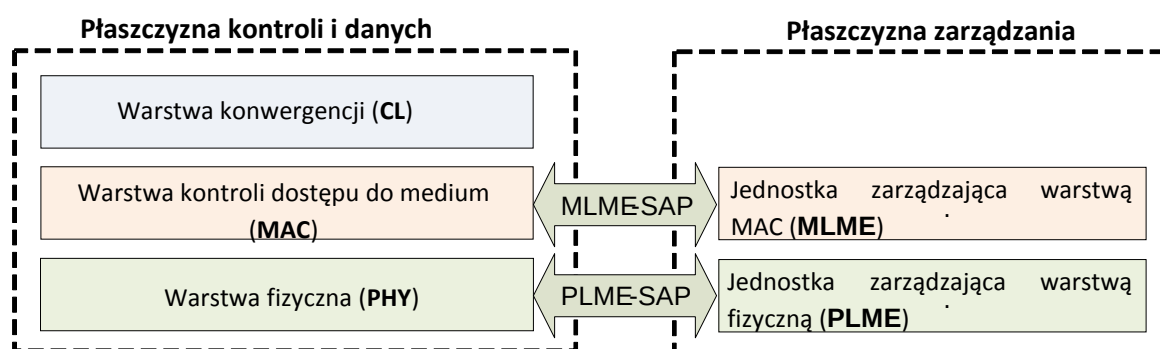
2 Opis ogólny

2.1 Wstęp

Niniejszy dokument jest specyfikacją rozwiązania dla PLC w paśmie CENELEC A za pomocą schematu modulacji OFDM.

2.2 Opis ogólny architektury

Rys. 1 przedstawia warstwy komunikacji i zakres niniejszej specyfikacji. Specyfikacja ta skupia się głównie na danych, kontroli i płaszczyźnie zarządzania.



Rys. 1 - Model referencyjny warstw protokołu stosowany w specyfikacji OFDM

CL klasyfikuje ruch kojarząc go z właściwym połączeniem MAC; warstwa ta wykonuje mapowanie dowolnego ruchu, aby prawidłowo znaleźć się w jednostkach MSDU. Może ona również obejmować funkcje kompresji nagłówka. Kilka SSCS jest definiowanych w celu akomodacji różnych rodzajów ruchu do jednostek MSDU.

Warstwa MAC zapewnia podstawowe funkcjonalności MAC dostępu systemowego, alokacji pasma, ustanawiania/zarządzania połączeniem i rozwiązania topologiczne.

Warstwa PHY przesyła i otrzymuje MPDU do i z węzłów sąsiadujących za pomocą ortogonalnych zwielokrotnień w dziedzinie częstotliwości (OFDM). OFDM wybrano jako technikę modulacji z powodu:

- jej naturalnych zdolności adaptacyjnych w obecności selektywnych częstotliwościowo kanałów (które są współdzielone, ale nieprzewidywalne z powodu wąskopasmowych zakłóceń lub przypadkowego zablokowania);
- jej odporności na hałas impulsowy, wynikający z przedłużonego czasu trwania symbolu i stosowanie FEC;
- jej zdolności do osiągnięcia wysokiej wydajności spektralnej za pomocą prostych implementacji nadawczo-odbiorczych.

Specyfikacja PHY, opisana w rozdziale 3, również wykorzystuje elastyczny schemat kodowania. Prędkości transmisji danych PHY mogą być dostosowywane do warunków kanału i hałasu przez MAC.

66 3 Warstwa fizyczna

67 3.1 Wstęp

68 Ten rozdział opisuje jednostkę zarządzającą warstwą fizyczną (PHY) dla schematu modulacji OFDM w
69 paśmie CENELEC A. Podmiot PHY wykorzystuje częstotliwości w paśmie 3 kHz do 95 kHz, jak określono w
70 normie EN 50065-1:2001+A1:2010 Sekcja 4.1. Wykorzystywanie częstotliwości w tym paśmie jest
71 zastrzeżone dla dystrybutorów energii elektrycznej i ich licencjobiorców. Powszechnie wiadomo, że
72 częstotliwości poniżej 40 kHz przejawia kilka problemów w typowych linii energetycznych NN. Na przykład:

- 73 • wielkości impedancji postrzegane przez nadajniki czasami wynoszą poniżej 1Ω , zwłaszcza dla węzłów
74 podstawowych znajdujących się przy transformatorach;
- 75 • kolorowy szum tła, który jest zawsze obecny w liniach energetycznych i powodowany przez
76 sumowanie wielu źródeł szumów o stosunkowo niskiej mocy, gwałtownie zwiększa swoją amplitudę
77 w kierunku niższych częstotliwości;
- 78 • pomieszczenia pomiarowe stanowią dodatkowy problem, ponieważ wiadome jest, że zachowania
79 klientów mają większy wpływ na własności kanału przy niskich częstotliwościach, tj. praca
80 wszelkiego rodzaju sprzętu domowego prowadzi do znacznych i nieprzewidywalnych zmiennych w
81 czasie zarówno charakterystyki funkcji transferu i scenariusza szumu.

82 W rezultacie specyfikacja PHY PRIME OFDM stosuje pasmo częstotliwości od 41,992 kHz do 88,867 kHz.
83 Osiąga się to poprzez modulację OFDM z sygnałem załadowanym na 97 równomiernie rozmieszczonych
84 podnośnych (96 danych i jedna pilotowa), przekazywanym w symbolach 2240 mikrosekund, z czego 192
85 mikrosekund składa się z krótkiego prefiksu cyklicznego.

86 Stosowana jest modulacja różnicowa w jednej z trzech możliwych konstelacji: DBPSK, DQPSK lub D8PSK. Tak
87 więc możliwe jest uzyskanie teoretycznie niekodowanych prędkości około 47 kb/s, 94 kb/s i 141 kb/s (bez
88 uwzględnienia narzutu prefiksu cyklicznego).

89 W celu uniknięcia wystąpienia długich sekwencji identycznych bitów, stosowany jest scrambler
90 synchroniczny.

91 Wreszcie, wraz z przeplotem bitowym stosowane będzie kodowanie splotowe przy 1/2 prędkości. Może być
92 ono wyłączone przez warstwy wyższe, jeśli kanał jest wystarczająco dobry i niezbędne są wyższe
93 przepustowości.

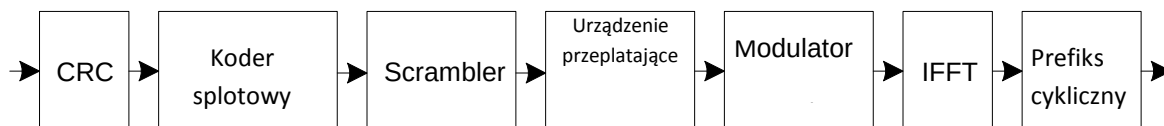
94 3.2 Omówienie

95 Po stronie nadajnika warstwa PHY otrzymuje MPDU z warstwy MAC i generuje ramkę PHY.

96 Przetwarzanie nagłówka PPDU pokazano na Rys. 2 i składa się ono z następujących kroków.

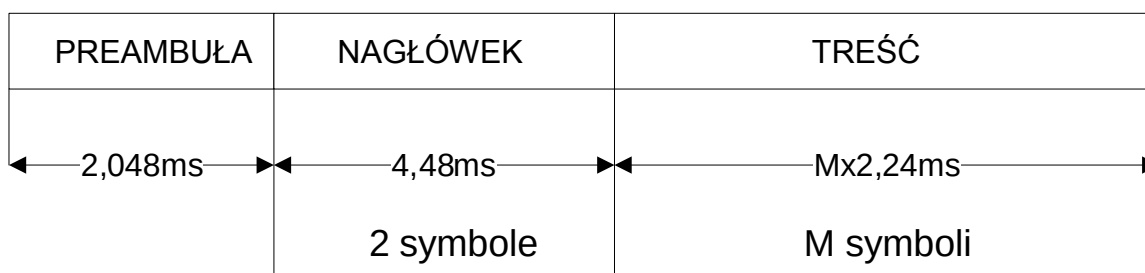
97 Kontrola CRC jest dołączana do nagłówka PHY (CRC dla treści jest dołączana przez warstwę MAC, więc PHY
98 nie dodaje już dodatkowych CRC). Następnie wykonywane jest kodowanie splotowe, jeśli włączona jest
99 opcjonalna korekcja FEC. (Należy zauważyć, że nagłówek PHY jest zawsze kodowany). Następnym krokiem
100 jest szyfrowanie, które jest realizowane zarówno dla nagłówka PHY i PPDU, niezależnie od tego, czy FEC jest
101 włączona. Jeśli korekcja FEC jest włączona, wyjście scramblera również jest przeplatane.

Szyfrowane (i przeplatane) bity są różnicowo modulowane za pomocą DBPSK, DQPSK lub D8PSK. Następnym krokiem jest OFDM, który obejmuje blok IFFT (Odwrotne szybkie przekształcenie Fouriera) i generator prefiksu cyklicznego. Gdy nagłówek i bity danych wprowadzane są do łańcucha pokazanego na Rys. 2, wyjściem generowania prefiksu cyklicznego jest łączenie symboli OFDM stanowiących odpowiednio nagłówek i treść PPDU. Część nagłówka zawiera dwa symbole OFDM, podczas gdy część treści zawiera M symboli OFDM. Wartość M sygnalizowana jest w nagłówku PHY, jak opisano w Punkcie 3.4.3.



Rys. 2 - Omówienie przetwarzania PPDU

Strukturę ramki PHY pokazano na Rys. 3. Każda ramka PHY rozpoczyna się preambułą trwającą 2,048 ms, po której następuje szereg symboli OFDM, każdy trwający 2,24 ms. Pierwsze dwa symbole OFDM przenoszą nagłówek ramki PHY, również nazywany w niniejszej specyfikacji nagłówkiem. Nagłówek jest również generowany przy zastosowaniu procesu podobnego do generowania treści, jak opisano w Punkcie 3.4.3. Pozostałe M symboli OFDM przenosi treść generowaną zgodnie z opisem w Punkcie 3.4.3. Wartość M jest sygnalizowane w nagłówku i jest co najwyżej równa 63.



Rys. 3 - Format ramki PHY

3.3 Parametry PHY

Tabela 1 podaje parametry częstotliwości i czasu stosowane w warstwie PHY OFDM PRIME. Parametry te są wspólne dla wszystkich konstelacji/kombinacji kodowania.

Uwaga Należy zauważyć, że w całym niniejszym dokumencie prędkości próbkowania 250 kHz i 512-punktowe FFT definiowane są dla potrzeb specyfikacji sygnałów OFDM i nie jest ich celem wskazywanie wymogu implementacji

Tabela 1 parametry częstotliwości i czasu w warstwie PHY OFDM PRIME

Parametr	Wartości
Zegar pasma podstawowego (Hz)	250000

Parametr	Wartości	
Rozstaw podnośnej (Hz)	488,28125	
Liczba podnośnych danych	84 (nagłówek)	96 (treść)
Liczba podnośnych pilotowych	13 (nagłówek)	1 (treść)
Interwał FFT (próbki)	512	
Interwał FFT (μ s)	2048	
Prefiks cykliczny (próbki)	48	
Prefiks cykliczny (μ s)	192	
Interwał symbolu (próbki)	560	
Interwał symbolu (μ s)	2240	
Okres preambuły (μ s)	2048	

126

127 Tabela 2 poniżej pokazuje szybkość transmisji danych PHY podczas transmisji treści oraz maksymalną
 128 długość MSDU dla różnych modulacji i kombinacji kodowania.

129 **Tabela 2 - parametry prędkości transmisji PHY oraz wielkości pakietów dla różnych modulacji i schematów kodowania**

	DBPSK		DQPSK		D8PSK	
	Wł.	Wył.	Wł.	Wył.	Wł.	Wył.
Kod splotowy (1/2)						
Liczba bitów informacji na podnośną N_{BPSC}	0,5	1	1	2	1,5	3
Liczba bitów informacji na symbol OFDM N_{BPS}	48	96	96	192	144	288
Szybkość transmisji danych pierwotnych (kb/s w przybliżeniu)	21,4	42,9	42,9	85,7	64,3	128,6
Maksymalna długość MSDU w 63 symbolami (w bitach)	3016	6048	6040	12096	9064	18144
Maksymalna długość MSDU w 63 symbolami (w bajtach)	377	756	755	1512	1133	<u>2268</u>

130

131 Tabela 3 pokazuje modulację i schemat kodowania oraz wielkości części nagłówka ramki PHY (patrz Punkt
 132 3.4.3).

133 **Tabela 3 - Parametry nagłówka**

	DBPSK
Kod splotowy (1/2)	Wł.
Liczba bitów informacji na podnośną N_{BPSC}	0,5
Liczba bitów informacji na symbol OFDM N_{BPS}	<u>42</u>

134

135 Zaleca się, aby wszystkie częstotliwości używane do generowania sygnału transmisji OFDM pochodziły z
136 jednej zadanej częstotliwości. Zegar systemowy powinien mieć maksymalną tolerancję ± 50 ppm, w tym
137 szeregowanie zadań.

138 3.4 Struktura preambuły, nagłówek i treści

139 3.4.1 Preambuła

140 Preambuła jest stosowana na początku każdej PPDU do celów synchronizacji. W celu zapewnienia
141 maksymalnej ilości energii, zamiast symboli OFDM stosowany jest stały sygnał obwiedni. Istnieje również
142 potrzeba, aby preambuła miała ruchliwość częstotliwości, która dopuści synchronizację w obecności
143 tłumienia selektywnego częstotliwościowo i, oczywiście, niezbędne są doskonałe aperiodyczne właściwości
144 autokorelacji. Liniowy sygnał zwężony spełnia wszystkie powyższe wymagania. Kształt fali preambuły
145 określa się jako:

$$146 S_{CH}(t) = A \cdot \text{rect}(t/T) \cdot \cos[2\pi(f_0 t + 1/2 \mu t^2)]$$

147
148 gdzie $T = 2048 \mu s$, $f_0 = 41992$ Hz (częstotliwość początkowa), $\mu = (f_t - f_0) / T$, przy częstotliwości końcowej $f_t =$
149 88867 Hz. Wybór parametru A określa średnią moc preambuły (podaną jako $A^2/2$), i został szczegółowo
150 omówiony w Punkcie 3.8

151 Funkcja *rect* jest definiowana jako:

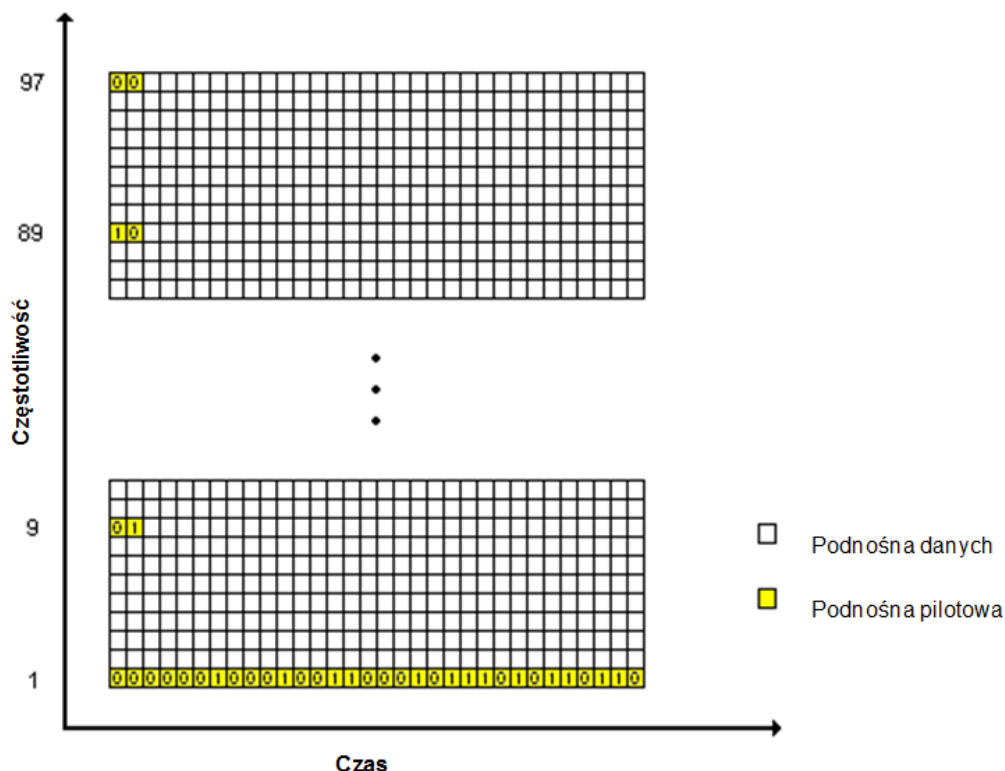
$$152 \begin{aligned} \text{rect}(t) &= 1, & 0 < t < 1 \\ \text{rect}(t) &= 0, & \text{otherwise} \end{aligned}$$

153 3.4.2 Struktura pilotowa

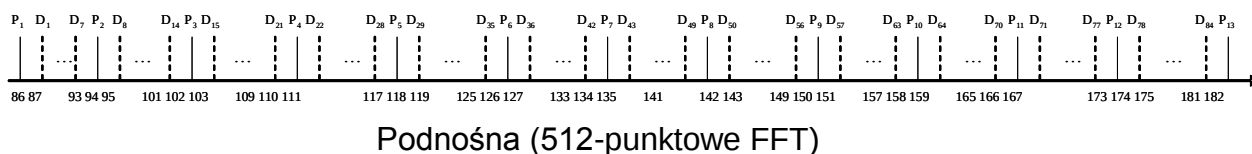
154 Po preambule następują dwa symbole OFDM składające się na nagłówek. Oba te symbole OFDM zawierają
155 13 podnośnych pilotowych, które można by wykorzystać do oszacowania błędu początku próbkowania oraz
156 wyrównania częstotliwości próbkowania.

157 Dla kolejnych symboli OFDM stosowana jest jedna podnośna pilotowa do zapewnienia odniesienia fazy dla
158 demodulacji w dziedzinie częstotliwości DPSK.

159 Alokacja częstotliwości podnośnej pilotowej pokazana została na Rys. 4 i Rys. 5, gdzie P_i jest i -tą podnośną
160 pilotową, a D_i jest i -tą podnośną danych.



Rys. 4 - Alokacja podnośnej pilotowej i podnośnej danych (symbole OFDM w por. do podnośnych)



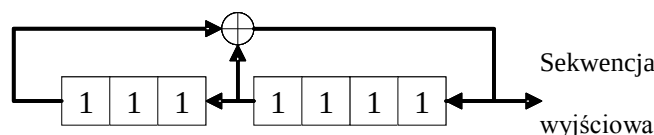
Rys. 5 - Alokacja częstotliwości podnośnej pilotowej i podnośnej danych wewnątrz nagłówka

Podnośne pilotowe są modulowane BPSK przez pseudolosową sekwencję binarną (pseudolosowość unika generowania linii widmowych). Faza podnośnej pilotowej kontrolowana jest przez ciąg pn, który stanowi cykliczne rozszerzenie ciągu 127-bitowego podanego jako:

$\text{Pref}_{0.126} = \{0,0,0,0,1,1,1,0,1,1,1,1,0,0,1,0,1,1,0,0,1,0,0,0,1,0,0,0,0,0,0,1,0,0,0,1,0,0,1,1,0,0,0,1,0,1,1,1,0,1,0,1,1,0,1,1,0,0,0,0,0,1,1,0,0,1,1,0,1,0,1,0,0,1,1,1,0,0,1,1,1,0,1,1,0,1,0,0,0,0,1,0,1,0,1,0,1,1,1,1,0,1,0,0,1,0,1,0,0,0,1,0,1,0,1,1,1,0,0,0,0,1,1,1,1,1,1,1\}$

W powyższym '1' oznacza przesunięcie fazowe 180°, a '0' oznacza przesunięcie fazowe 0°. Dla każdej podnośnej pilotowej użyty będzie jeden bit ciągu, począwszy od pierwszej podnośnej pilotowej w pierwszym symbolu OFDM, następnie kolejnej podnośnej pilotowej, itd. Ten sam proces stosowany jest dla drugiego symbolu OFDM. Dla kolejnych symboli OFDM dla podnośnej pilotowej stosowany jest jeden element ciągu (patrz Rys. 5).

Ciąg pn jest generowany przez scrambler określony na Rys. 6, gdy używany jest stan początkowy „same jedynek”.



Rys. 6 - LFSR do stosowania w generowaniu ciągu pilotowego

Wczytywanie ciągu pn powinno być inicjowane na początku każdej jednostki PPDU, zaraz po preambule.

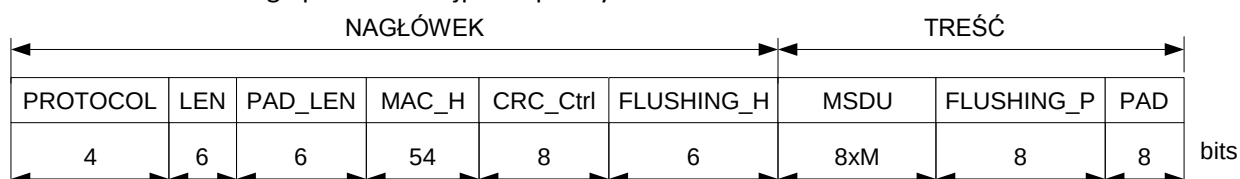
3.4.3 Nagłówek i treść

Nagłówek składa się z dwóch symboli OFDM, które zawsze są wysyłane za pomocą modulacji DBPSK i włączonej korekcji FEC (kodowania splotowego). Jednakże treść jest modulowana kluczowaniem DBPSK, DQPSK lub D8PSK, w zależności od konfiguracji przez warstwę MAC. Warstwa MAC może wybrać najlepszy schemat modulacji korzystając z informacji z błędów z poprzednich transmisji do tego samego odbiornika (tych samych odbiorników) lub za pomocą sprzężenia zwrotnego SNR. Tak więc system będzie konfigurować się dynamicznie w celu zapewnienia najlepszego kompromisu pomiędzy przepustowością i wydajnością komunikacji. Obejmuje to podejmowanie decyzji, czy FEC (kodowanie splotowe) będzie używane, czy nie.

Uwaga: Optymalizacja i docelowy współczynnik błędów dla wyboru modulacji i schematu FEC pozostawione są do indywidualnych wdrożeń

Pierwsze dwa symbole OFDM w PPDU (odpowiadające nagłówkowi) składają się z 84 podnośnych danych i 13 podnośnych pilotowych. Po nagłówku każdy symbol OFDM w treści przenosi 96 podnośnych danych i jednej podnośnej pilotowej. Każda podnośna danych przenosi 1, 2 lub 3 bity.

Strumień bitów z każdego pola musi najpierw przesyłać nzb.



Rys. 7 - PPDU: nagłówek i treść (bity przesłane przed kodowaniem)

- **NAGŁÓWEK:** Każda jednostka PPDU zawiera informacje na temat zarówno warstwy PHY jak i MAC. Aby uniknąć dwuznaczności, nagłówek MAC jest zawsze nazywany „nagłówkiem MAC”. Nagłówek PHY może być również nazywany po prostu „nagłówkiem”. Składa się on z następujących pól:
 - **PROTOKÓŁ:** zawiera schemat transmisji treści. Dodawany przez warstwę PHY.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
DBPSK	DQPSK	D8PSK	RES	DBPSK_F	DQPSK_F	D8PSK_F	RES	RES	RES	RES	RES	RES	RES	RES	RES
 - Gdzie RES oznacza Zarezerwowany – „Reserved”, a sufiks „_F” oznacza, że korekcja FEC jest włączona.
 - **LEN:** określa długość treści (po kodowaniu) w symbolach OFDM. Dodawany przez warstwę PHY.
 - **PAD_LEN:** określa długość pola PAD (przed kodowaniem) w bajtach. Dodawany przez warstwę PHY.

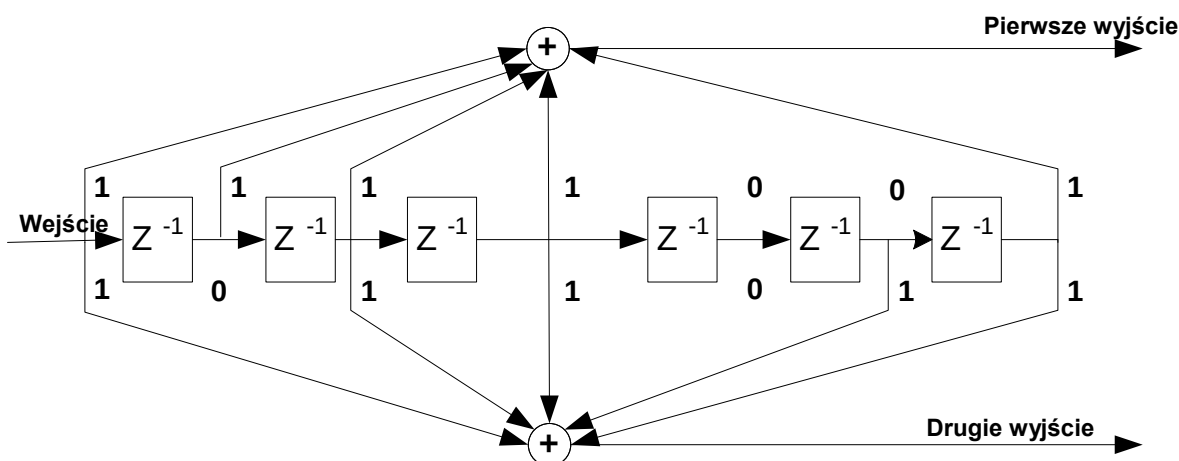
- MAC_H: Nagłówek warstwy MAC. Znajduje się on wewnątrz symboli nagłówka w celu ochrony zawartych w nim informacji. Należy zauważyć, że nagłówek MAC generowany jest przez warstwę MAC i tylko pierwsze 54 bity nagłówka MAC osadzone jest w warstwie PHY.
- CRC_Ctrl: the CRC_Ctrl(m), $m = 0..7$, zawiera sumę kontrolną CRC w polach PROTOKÓŁ, LEN, PAD_LEN i MAC_H (PD_Ctrl). Forma wielomianowa PD_Ctrl wyraża się następująco:

$$\sum_{m=0}^{69} PD_{Ctrl}(m)x^m$$

- Suma kontrolna obliczana jest w następujący sposób: reszta z dzielenia PD_Ctrl przez formy wielomianowe $x^8 + x^2 + x + 1$ CRC_Ctrl(m), gdzie CRC_Ctrl(0) jest najmniej znaczącym bitem. Wielomian generujący to bardzo znany CRC-8_ATM. Część przykładów pokazano w Załącznik A. Suma dodawana jest przez warstwę PHY.
- FLUSHING_H: bity resetujące niezbędne do kodowania splotowego. Wszystkie bity w tym polu ustawione są na zero, aby zresetować koder splotowy. Dodawany przez warstwę PHY.
- TREŚĆ:
 - MSDU: Niekodowana jednostka danych usługi warstwy MAC.
 - FLUSHING_P: bity resetujące niezbędne do kodowania splotowego. Wszystkie bity w tym polu ustawione są na zero, aby zresetować koder splotowy. Pole to istnieje jedynie, gdy włączona jest korekcja FEC.
 - PAD: Pole wypełnienia. W celu zapewnienia, że ilość (kodowanych) bitów generowana w tej treści wypełnia liczbę całkowitą symboli OFDM, przed kodowaniem do treści dodane mogą zostać bity wypełnienia. Wszystkie bity wypełnienia muszą być ustawione na zero.

3.5 Koder splotowy

Strumień niekodowanych bitów może przejść przez kodowanie splotowe, aby utworzyć strumień bitów zakodowanych. Koder splotowy działa przy 1/2 prędkości i ograniczeniu długości $K = 7$ i wielomianach generujących kodu 1111001 i 1011011. Na początku każdej transmisji PPDU stan kodera ustawiany jest na zero. Jak widać na Rys. 8, na końcu bitów nagłówka wstawiono osiem zer, aby zrestartować koder i przywrócić stan do zera. Podobnie, jeśli kodowanie splotowe stosowane jest dla treści, sześć bitów zerowych wstawianych jest na końcu strumienia bitów wejściowych, aby zapewnić powrót stanu kodera do zera na końcu treści. Diagram blokowy kodera pokazano na Rys. 9.



Rys. 8 - Koder splotowy

241 3.6 Scrambler

242 Blok scramblera losuje strumień bitów, tym samym zmniejsza współczynnik szczytu na wyjściu IFFT, gdy
243 długi strumień zer lub jedynek występuje w nagłówku lub treści po kodowaniu (jeśli w ogóle). Mieszanie
244 jest zawsze wykonywane niezależnie od konfiguracji modulacji i kodowania.

245 Blok scrablera wykonuje alternatywę wykluczającą wejściowego strumienia bitów przez ciąg pseudolosowy
246 pn, uzyskiwany przez rozszerzenie cykliczne 127-elementowego ciągu podane jako:

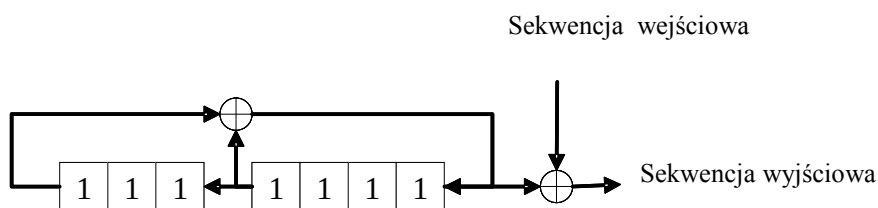
247 Pref_{0..126}=

```

248 {0,0,0,0,1,1,1,0,1,1,1,1,0,0,1,0,1,1,0,0,1,0,0,0,1,0,0,0,0,0,1,0,0,0,1,0,0,1,1,0,0,0,1,0,1,1,1,0,1,0,1,1,0,1,1,0,0,
249 0,0,0,1,1,0,0,1,1,0,1,0,1,0,0,1,1,1,0,0,1,1,1,0,1,1,0,1,0,0,0,0,1,0,1,0,1,0,1,1,1,1,0,1,0,0,1,0,1,0,0,0,1,1,0,1
250 ,1,1,0,0,0,1,1,1,1,1,1,1}

```

251 **Uwaga:** Powyższy 127-elementowy ciąg może być generowany przez LFSR określony na Rys. 9, gdy
252 stosowany jest stan początkowy „same jedyńki”.



Rys. 9 - LFSR do stosowania w bloku scramblera

255 Wczytywanie ciągu pn powinno być inicjowane na początku każdej jednostki PPDU, zaraz po preambule.

256 **3.7 Urządzenie przeplatające**

Ze względu na blaknięcie częstotliwości (zakłócenia wąskopasmowe) typowych kanałów przesyłowych, podnośne OFDM są zazwyczaj otrzymywane przy różnych amplitudach. Głębokie zaniki w widmie mogą powodować spadek niezawodności grup podnośnych, co powoduje występowanie błędnych bitów w seriach, a nie losowo. Jeśli (i tylko jeśli) kodowanie jest stosowane zgodnie z opisem w 3.4, przeplatanie stosuje się w celu zrandomizowania występowania błędnych bitów przed dekodowaniem. Przy nadajniku zakodowane bity są permutowane w określony sposób, co zapewnia, że sąsiadujące bity są oddzielone po przeplocie o kilka bitów.

264 Niech $N_{\text{CBPS}} = 2 \times N_{\text{NBPS}}$ będzie liczbą zakodowanych bitów na symbol OFDM w przypadku stosowania
265 kodowania spłotowego. Wszystkie zakodowane bity muszą być przeplatane blokowym urządzeniem
266 przeplatającym z rozmiarem bloku odpowiadającym N_{CBPS} . Urządzenie przeplatające zapewnia, że
267 sąsiadujące zakodowane bity zmapowane są na niesąsiadujące podnośne danych. Niech $v(k)$, z $k = 0, 1, \dots,$
268 $N_{\text{CBPS}} - 1$, będzie wektorowymi bitami kodowanymi przy wejściu do urządzenia przeplatającego. Wektor $v(k)$
269 jest przekształcany w wektor przeplatania $w(i)$, z $i = 0, 1, \dots, N_{\text{CBPS}} - 1$ przez blokowe urządzenie przeplatające
270 w następujący sposób:

$$w((N_{\text{CBPS}}/s) \times (k \bmod s) + \text{floor}(k/s)) = v(k) \quad k = 0, 1, \dots, N_{\text{CBPS}} - 1$$

Wartość s jest określana przez liczbę zakodowanych bitów na podnośną, $N_{CBPSC}=2 \times N_{BPSC}$. N_{CBPSC} odnosi się do N_{CBPS} , tak że $N_{CBPS}=96 \times N_{CBPSC}$ (treść), a $N_{CBPS}=84 \times N_{CBPSC}$ (nagłówek)

274 $s = 8 \times (1 + \text{floor}(N_{\text{CBPSC}}/2))$ dla treści i

275 $s = 7$ dla nagłówka.

276 Przy odbiorniku urządzenie odprzeplatające wykonuje operację odwrotną. Stąd, jeśli $w'(i)$, z $i = 0, 1, \dots, N_{\text{CBPS}} - 1$,
 277 jest wektorową wartością wejściową odprzeplatania, wektor $w'(i)$ przekształcany jest w wektor
 278 odprzeplatania $v'(k)$, z $k = 0, 1, \dots, N_{\text{CBPS}} - 1$, przez blokowe urządzenie odprzeplatające.

279 $v'(s \times i - (N_{\text{CBPS}} - 1) \times \text{floor}(s \times i / N_{\text{CBPS}})) = w'(i) \quad i = 0, 1, \dots, N_{\text{CBPS}} - 1$

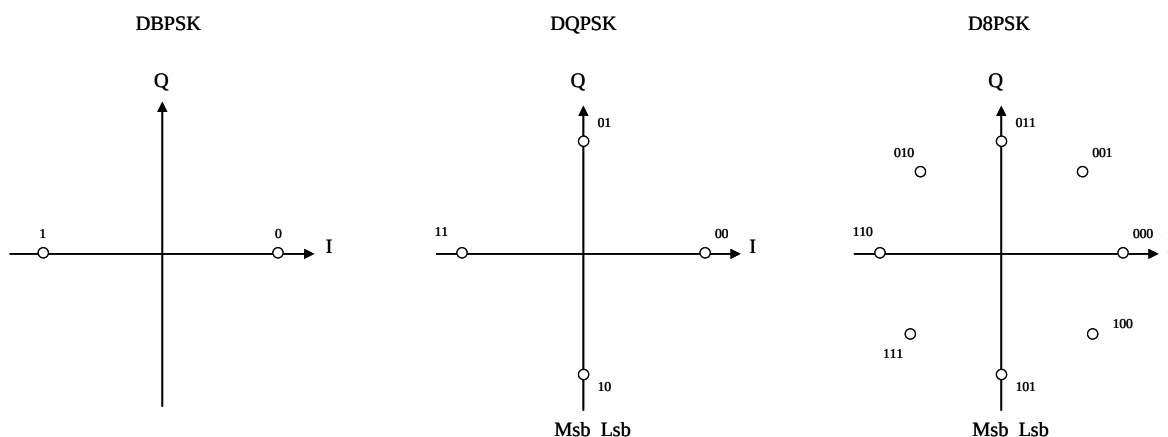
280 Opisowe tabele wykazujące permutacje indeksu można znaleźć w Załącznik C.

281 3.8 Modulacja

282 Treść PPDU modulowana jest jako sygnał różnicowego kluczowania wielu nośnych z przesunięciem fazy z
 283 jedną podnośną pilotową i 96 podnośnymi danych, które składają się z 96, 192 lub 288 bitów na symbol.
 284 Nagłówek modulowany jest przez DBPSK z 13 podnośnymi pilotowymi i 84 podnośnymi danych, które
 285 składają się z 84 bitów na symbol.

286 Strumień bitów pochodzący z urządzenia przeplatającego dzieli się na grupy M-bitów, gdzie pierwszy bit
 287 grupy M jest najbardziej znaczącym bitem (nzb).

288 Przede wszystkim wykonywana jest modulacja różnicowa w dziedzinie częstotliwości. Rys. 10 pokazuje
 289 mapowanie DBPSK, DQPSK i D8PSK:



Rys. 10 - Mapowanie DBPSK, DQPSK i D8PSK

292 Kolejne równanie definiuje konstelację M-owego kluczowania DPSK faz M:

$$293 \quad s_k = A e^{j\theta_k}$$

294 Gdzie:

- 295 • k jest indeksem częstotliwości reprezentującym k -tą podnośną w symbolu OFDM . $k = 1$ odpowiada
 296 podnośnej pilotowej odniesienia fazy.
- 297 • s_k jest wartością wyjściową modulatora (liczbą zespoloną) dla k -tej podanej podnośnej.
- 298 • θ_k oznacza bezwzględną fazę sygnału modulowanego i otrzymuje się ją w następujący sposób:
- 299 • $\theta_k = (\theta_{k-1} + (2\pi / M) \Delta b_k) \bmod 2\pi$

- Równanie to ma zastosowanie do $k > 1$ treści, $k = 1$ jest podnośną pilotową odniesienia fazy. Kiedy nagłówek jest przesyłany, podnośna pilotowa alokowana w k -tej podnośnej, stosowana jest jako odniesienie fazy dla danych alokowanych w $k + 1$ -tej podnośnej.
- $\Delta b_k \in \{0, 1, \dots, M-1\}$ oznacza informacje zakodowane w przyroście fazy, w formie dostarczonej przez koder konstelacji.
- $M = 2, 4$, lub 8 w przypadku DBPSK, DQPSK lub D8PSK odpowiednio.
- A jest parametrem kształtowania i stanowi promień pierścienia od środka konstelacji. Wartość A określa moc w każdej podnośnej, a tym samym średnią moc przesyłaną w symbolach nagłówka i treści.

Symbol OFDM można wyrazić w formie matematycznej:

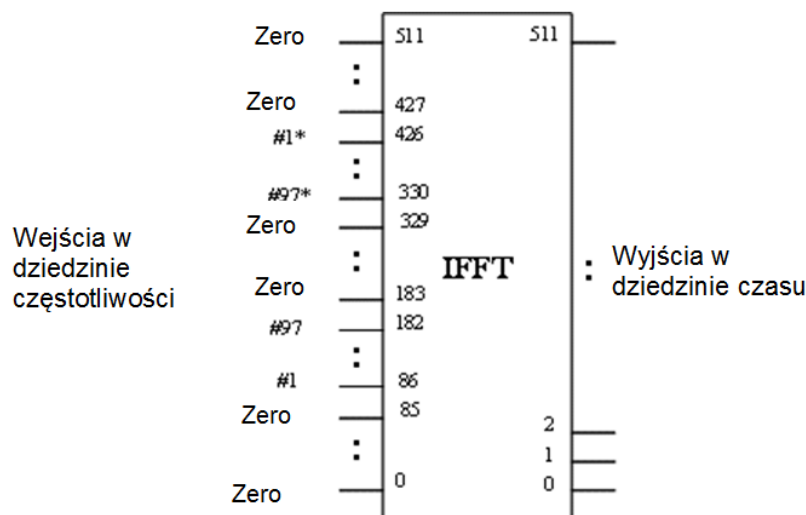
$$c_i(n) = \left\{ \sum_{k=86}^{182} s(k-85, i) \exp\left(\frac{j2\pi}{512} k(n - N_{CP})\right) + \sum_{k=330}^{426} s^*(427-k, i) \exp\left(\frac{j2\pi}{512} k(n - N_{CP})\right) \right\}$$

- i jest indeksem czasu reprezentującym i -ty symbol OFDM; $i = 0, 1, \dots, M+1$.
- $s(k, i)$ jest złożoną wartością z bloku modulacji podnośnej, a symbol $*$ oznacza sprzężenie zespolone.
- n jest indeksem próbnym; $0 \leq n \leq 559$.

Uwaga 1: Należy zauważyć, że $c_i(n+512) = c_i(n)$, tak więc pierwszych 48 próbek powyżej jest równych ostatnim 48 próbkom, a tym samym stanowi prefiks cykliczny. Niektóre próbki z prefiksu cyklicznego mogą być stosowane do okienkowania właściwego dla dostawcy.

Uwaga 2: Chociaż dokładne dane dotyczące okienkowania pozostawiono indywidualnym wdrożeniom, należy zauważyć, że urządzenia certyfikowane do użycia z PRIME muszą spełniać wartości graniczne EVM określone przez testy certyfikacyjne zgodnie z procedurą pomiarową EVM wspomnianą w Załącznik B

Jeśli stosowane jest 512-punktowe IFFT, 96 podnośnych powinno być mapowane zgodnie z Rys. 11. Symbol $*$ stanowi sprzężenie zespolone.



Rys. 11 - Mapowanie podnośnej

Po odwrotnym szybkim przekształceniu Fouriera symbol jest cyklicznie rozszerzany o 48 próbek w celu utworzenia prefiksu cyklicznego (N_{CP}).

3.9 Parametry elektryczne nadajnika

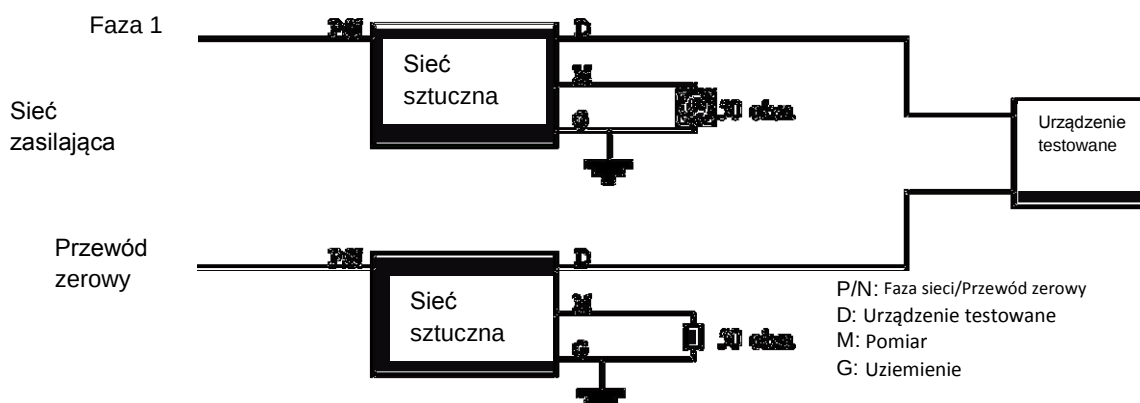
3.9.1 Ogólne

Następujące wymagania dotyczące ustanawiania minimalnych wymagań technicznych nadajnika dla interoperacyjności i odpowiedniego działania nadajnika.

3.9.2 PSD nadajnika

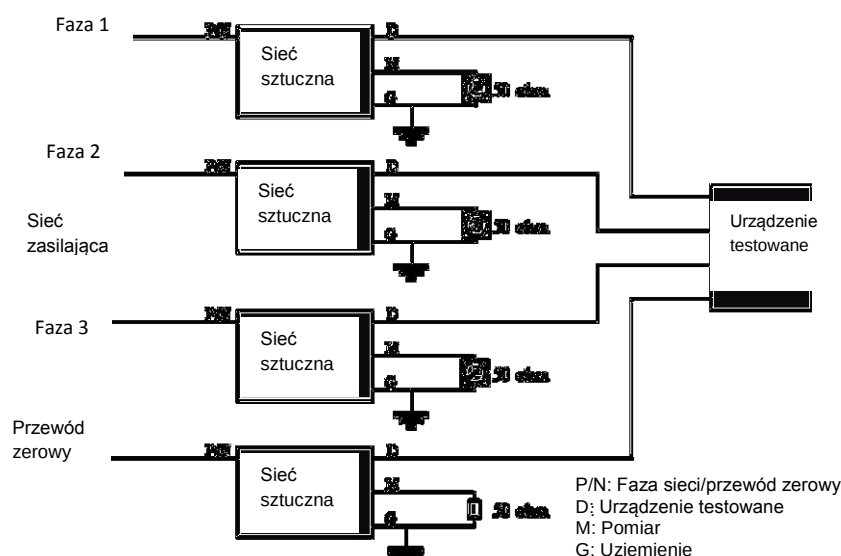
Specyfikacje nadajnika będą mierzone zgodnie z następującymi warunkami i konfiguracją:

Dla urządzeń jednofazowych pomiar zostanie dokonany na fazie lub w warunkach neutralnych zgodnie z Rys. 12.



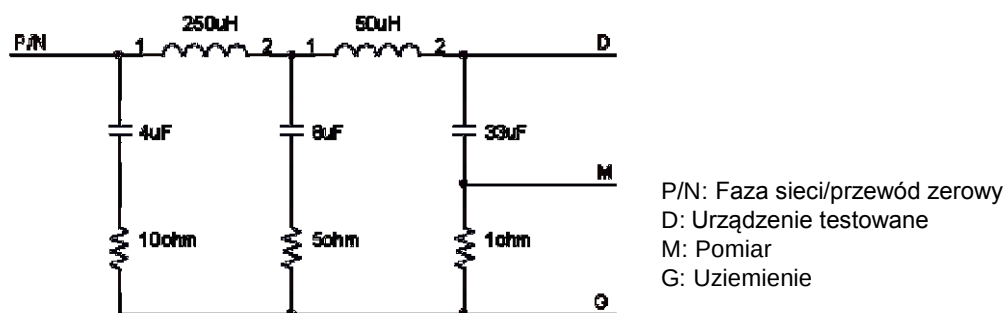
Rys. 12 – Konfiguracja pomiarów (jedna faza)

Dla urządzeń trójfazowych, które transmitują na wszystkich trzech fazach jednocześnie, pomiary powinny być przeprowadzane we wszystkich trzech fazach zgodnie z Rys. 13. Pomiary przewodu zerowego nie są wymagane.



Rys. 13 – Konfiguracja pomiarów (trzy fazy)

Sieć sztuczna na Rys. 12 i Rys. 13 została pokazana na Rys. 14. Opiera się ona na normie EN 50065-1:2001. Kondensator 33 μ F i opornik 1 Ω wprowadzono tak, aby sieć miała impedancję 2 Ω w zadanym paśmie częstotliwości.



Rys. 14 – Sieć sztuczna

Wszystkie napięcia wyjściowe nadajnika są określone jako napięcia mierzone przy terminalu liniowym w odniesieniu do terminala neutralnego. Zgodnie z tym wartości uzyskane z urządzenia pomiarowego należy zwiększyć o 6 dB (dzielnik napięcia w stosunku 1/2).

Wszystkie urządzenia będą sprawdzone pod kątem spełniania wymagań PSD w pełnym zakresie temperatury, która zależy od typu węzła:

- Węzły podstawowe w zakresie -40 °C do +70 °C
- Węzły serwisowe w zakresie od -25 °C do +55 °C

Wszystkie testy będą przeprowadzone w normalnych warunkach natężenia wymiany.

We wszystkich przypadkach PSD musi być zgodna z przepisami obowiązującymi w kraju stosowania systemu.

359 W przypadku tylko jednej fazy wzmacniacz mocy powinien móc wprowadzić poziom ostatecznego sygnału
360 w węzle transmitującym (parametr S1) w wielkości 120 dBμVrms (1 Vrms). To może być jeden z dwóch
361 scenariuszy: testowane urządzenie jest podłączone do jednej fazy, jak pokazano na Rys. 12 albo do trzech
362 faz, jak pokazano na Rys. 13, ale napędza tylko jedną fazę na raz. W obu przypadkach połączenie odbywa
363 się przez sieć sztuczną z Rys. 14.

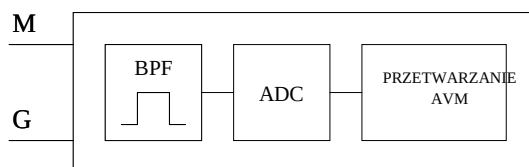
364 Dla urządzeń trójfazowych wprowadzanych równolegle do wszystkich trzech faz poziom ostatecznego
365 sygnału powinien wynosić 114 dBμVrms (0,5 Vrms).

366 **Uwaga 1:** We wszystkich powyższych przypadkach należy zwrócić uwagę, że w urządzeniach pomiarowych
367 występuje tłumienność wtrąceniowa. W szczególności w konfiguracji urządzeń jednofazowych mierzone
368 napięcie wynosi 6 dB poniżej właściwego poziomu sygnału i będzie równy 114 dBuV, gdy właściwy poziom
369 wynosi 120 dBuV. Podobnie, gdy urządzenie podłączone jest do trzech faz, mierzony poziom sygnału
370 wyniesie 12 dB poniżej właściwego poziomu sygnału. Tak więc sygnał 114 dBuV wprowadzony równocześnie
371 w trzy fazy będzie mierzony jako 102 dBuV na każdym z trzech metrów Rys. 13.

372 **Uwaga 2:** Zastosowanie mogą mieć ograniczenia regionalne, np. w sprawie mocy biernej z miernika, w tym
373 modemu OFDM PRIME. Przepisy te mogą mieć wpływ na interfejs PLC i należy się do nich stosować.

374 3.9.3 Wielkość wektora błędu (EVM)

375 Jakość wprowadzonego sygnału w odniesieniu do impedancji sztucznych sieci musi być mierzona w celu
376 sprawdzenia urządzenia nadajnika. W związku z powyższym należy zastosować analizę wektorową, która
377 zapewnia pomiary wielkości wektora błędu (EVM), patrz Załącznik B dla definicji EVM. Konfiguracja testu
378 opisana na Rys. 12 i Rys. 13 powinna być stosowana w przypadku urządzeń jednofazowych i trójfazowych
379 przesyłających równocześnie na wszystkich fazach odpowiednio.



380

381

Rys. 15 – Pomiar EVM (diagram blokowy)

382 Pomiar EVM musi obejmować filtr środkowoprzepustowy z tłumieniem 40 db przy 50 Hz, które zapewnia
383 antialiasing dla przetwornika analogowo-cyfrowego ADC. Minimalne osiągi ADC to 1 MSPS, efektywna
384 liczba bitów = 14. Tętnienia i opóźnienia filtra środkowoprzepustowego należy uwzględnić w obliczeniach
385 EVM.

386 3.9.4 Przeprowadzone ograniczenia zakłóceń

387 Zastosowanie mogą mieć przepisy lokalne. Na przykład w Europie nadajniki muszą być zgodne z
388 najwyższymi dopuszczalnymi poziomami emisji i emisji pasożytniczych określonych w EN50065 -1:2001 dla
389 emisji przeprowadzonych w sieciach AC w paśmie od 3 kHz do 9 kHz i od 95 kHz do 30 MHz. Rozporządzenia
390 europejskie również wymagają, aby nadajnik i odbiornik były zgodne z wartościami granicznymi impedancji
391 określonymi w EN 50065 -7:2001 w zakresie od 3 kHz do 148,5 kHz.

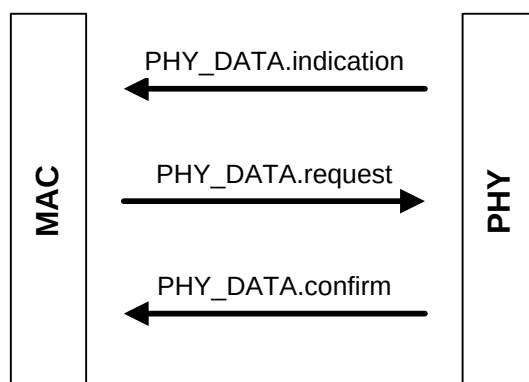
3.10 Specyfikacja usługi PHY

3.10.1 Ogólne

Warstwa PHY powinna mieć pojedynczy 20-bitowy zegar zwiększany w krokach co 10 μ s. Zegar odlicza od 0 do 1048575, a następnie wraca do 0. W związku z tym okres tego zegara wynosi 10,48576 sekundy. Zegar nigdy nie jest zatrzymywany, ani zerowany. Czas mierzony przez ten zegar to czas stosowany w niektórych prymitywach PHY do wskazywania określonych chwil w czasie.

3.10.2 Prymitywy płaszczyzny danych PHY

3.10.2.1 Ogólne



Rys. 16 – Omówienie prymitywów PHY

Prymityw żądania przekazywany jest z warstwy PHY do MAC w celu żądania zainicjowania usługi.

Prymitywy wskazania i potwierdzenia przekazywane są z warstwy PHY do MAC w celu wskazania wewnętrznego zdarzenia PHY, które ma znaczenie dla MAC. To zdarzenie może być logicznie powiązane ze zdalnym zgłoszeniem usługi lub może być spowodowane przez zdarzenia wewnętrzne PHY.

3.10.2.2 PHY_DATA.request

3.10.2.2.1 Funkcja

Prymityw PHY_DATA.request przekazywany jest do warstwy PHY w celu zgłoszenia wysłania PPDU do jednej lub więcej jednostek PHY za pomocą procedur transmisji PHY. Pozwala on również na ustawienie czasu, w którym transmisja musi zostać uruchomiona.

3.10.2.2.2 Struktura

Semantyka tego prymitywu przedstawia się następująco:

PHY_DATA.request{MPDU, Length, Level, Scheme, Time}.

Parametr MPDU określa jednostkę danych protokołu MAC przekazywaną przez jednostkę warstwy PHY. Jest on obowiązkowy dla implementacji w celu wyrównania bajtowego MPDU w SAP warstwy PHY. Oznacza to 2 dodatkowe bity (z powodu niewyrównanego pod względem bitów charakteru nagłówka warstwy MAC) umieszczane na początku nagłówka.

- 418 Parametr długości *Length* określa długość MPDU w bajtach. Długość wynosi 2 bajty.
- 419 Parametr poziomu *Level* określa poziom wyjściowy sygnału, zgodnie z którym warstwa PHY przesyła MPDU.
420 Może on przyjąć jedną z ośmiu wartości:
- 421 0: Maksymalny poziom wyjściowy (MOL)
- 422 1: MOL -3 dB
- 423 2: MOL -6 dB
- 424 ...
- 425 7: MOL -21 dB
- 426 Parametr schematu *Scheme* określa schemat transmisji stosowany dla MPDU. Może przyjąć on dowolną z
427 następujących wartości :
- 428 0: DBPSK
- 429 1: DQPSK
- 430 2: D8PSK
- 431 3: Nieużywany
- 432 4: DBPSK + kod splotowy
- 433 5: DQPSK + kod splotowy
- 434 6: D8PSK + kod splotowy
- 435 7: Nieużywany
- 436 Parametr czasu *Time* określa chwilę w czasie, w której przesłana ma zostać jednostka MPDU. Wyrażany jest
437 on w 10-tkach μs i może przyjmować wartości od 0 do $2^{20}-1$.
- 438 Należy zauważyć, że parametr *Time* powinien być obliczony przez MAC biorąc pod uwagę aktualny czas
439 PHY, który można uzyskać za pomocą prymitywu PHY_timer.get. Warstwa MAC powinna uwzględnić fakt,
440 że żadnej części PPDU nie można przesłać podczas szczelin sygnału i w okresach CFP przyznawanych innym
441 urządzeniom w sieci. Jeśli parametr czasu jest ustawiony tak, że powyższe zasady są naruszane, warstwa
442 PHY zwróci błąd w PHY_Data.confirm.
- 443 **3.10.2.2.3 Użycie**
- 444 Prymityw generowany jest przez jednostkę warstwy MAC gdy dane mają zostać przesłane do równorzędnej
445 jednostki MAC.
- 446 Odbiór tego prymitywu spowoduje, że jednostka PHY wykona wszystkie właściwe dla PHY działania i
447 przekaże poprawnie sformułowaną jednostkę PPDU do jednostki sprzęgającej linii energetycznej celem
448 przesłania do jednostki równorzędnej warstwy PHY. Kolejna transmisja powinna rozpocząć się gdy atrybut
449 czasu *Time* będzie równy wartości Timer.

450 3.10.2.3 PHY_DATA.confirm

451 3.10.2.3.1 Funkcja

452 Prymityw PHY_DATA.confirm ma jedynie znaczenie lokalne i zapewnia odpowiednią odpowiedź dla
453 prymitywu PHY_DATA.request. Prymityw PHY_DATA.confirm mówi jednostce warstwy MAC czy MPDU
454 poprzedniego prymitywu PHY_DATA.request została poprawnie wysłana czy nie.

455 3.10.2.3.2 Struktura

456 Semantyka tego prymitywu przedstawia się następująco:

457 PHY_DATA.confirm{*Result*}.

458 Parametr wyniku *Result* jest używany do przekazywania informacji o stanie z powrotem do lokalnej
459 jednostki wnioskującej. Jest on używany do wskazania powodzenia lub niepowodzenia poprzedniego
460 prymitywu PHY_DATA.request. Niektóre wyniki będą standardowe dla wszystkich wdrożeń:

461 0: Powodzenie.

462 1: Za późno. Czas przeznaczony na transmisję upłynął.

463 2: Nieprawidłowa *Długość*.

464 3: Nieprawidłowy *Schemat*.

465 4: Nieprawidłowy *Poziom*.

466 5: Przepełnienie bufora.

467 6: Kanał zajęty.

468 7-255: Zastrzeżony.

469 3.10.2.3.3 Użycie

470 Prymityw jest generowany w odpowiedzi na PHY_DATA.request.

471 Zakłada się, że warstwa MAC posiada wystarczające informacje, aby skojarzyć prymityw potwierdzenia
472 (confirm) z odpowiednim prymitywem wniosku (request).

473 3.10.2.4 PHY_DATA.indication

474 3.10.2.4.1 Funkcja

475 Ten prymityw określa transfer danych z jednostki warstwy PHY do jednostki warstwy MAC.

476 3.10.2.4.2 Struktura

477 Semantyka tego prymitywu przedstawia się następująco:

478 PHY_DATA.indication{*PSDU*, *Length*, *Level*, *Scheme*, *Time*}.

479 Parametr *PSDU* określa jednostkę danych usługi PHY odbieraną przez lokalną jednostkę warstwy PHY. Jest
 480 on obowiązkowy dla implementacji w celu wyrównania bajtowego MPDU w SAP warstwy PHY. Oznacza to 2
 481 dodatkowe bity (z powodu niewyrównanego pod względem bitów charakteru nagłówka warstwy MAC)
 482 umieszczane na początku nagłówka.

483 Parametr długości *Length* określa długość PSDU w bajtach. Długość wynosi 2 bajty.

484 Parametr poziomu *Level* określa poziom sygnału, zgodnie z którym warstwa PHY podbiera PSDU. Może on
 485 przyjąć jedną z szesnastu wartości:

486 0: ≤ 70 dBuV

487 1: ≤ 72 dBuV

488 2: ≤ 74 dBuV

489 ...

490 15: > 98 dBuV

491 Parametr *Scheme* określa schemat, zgodnie z którym odbierana jest jednostka PSDU. Może przyjąć on
 492 dowolną z następujących wartości :

493 0: DBPSK

494 1: DQPSK

495 2: D8PSK

496 3: Nieużywany

497 4: DBPSK + kod splotowy

498 5: DQPSK + kod splotowy

499 6: D8PSK + kod splotowy

500 7: Nieużywany

501 Parametr czasu *Time* to czas odbierania preambuły skojarzonej z PSDU.

502 3.10.2.4.3 Użycie

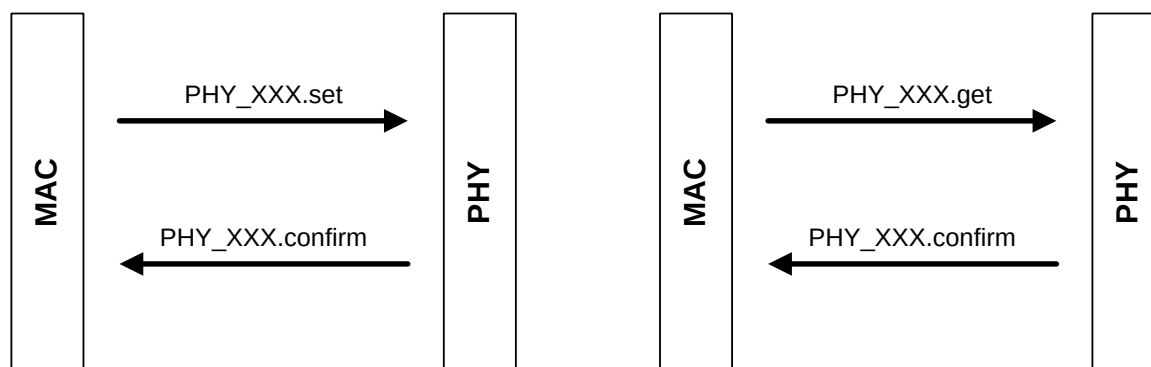
503 Prymityw PHY_DATA.indication jest przekazywany z jednostki warstwy PHY do jednostki warstwy MAC w
 504 celu wskazania dostarczenia prawidłowej PPDU.

505 3.10.3 Prymitywy płaszczyzny kontrolnej PHY

506 3.10.3.1 Ogólne

507 Rys. 17 pokazuje strukturę tworzenia prymityw płaszczyzny kontrolnej PHY. Każdy prymityw może mieć
 508 pola „set”, „get” i „confirm”. Tabela 4 poniżej podaje prymitywy płaszczyzn kontrolnej i pola skojarzone z

każdym z nich. Każdy szereg jest prymitywem płaszczyzny kontrolnej. „X” w kolumnie oznacza, że powiązane pole jest używane w prymitywach opisanych w tym wierszu.



Rys. 17 – Omówienie prymitywów płaszczyzny kontrolnej PHY

Tabela 4 - Pola skojarzone z prymitywami płaszczyzny kontrolnej warstwy PHY

Pole	set (ustaw)	get (uzyskaj)	confirm (zatwierdź)
PHY_AGC	X	X	X
PHY_Timer		X	X
PHY_CD		X	X
PHY_NL		X	X
PHY_SNR		X	X
PHY_ZCT		X	<u>X</u>

3.10.3.2 PHY_AGC.set

3.10.3.2.1 Funkcja

Prymityw PHY_AGC.set jest przekazywany do jednostki warstwy PHY przez warstwę MAC w celu ustawienia trybu automatycznego wzmocnienia warstwy PHY.

3.10.3.2.2 Struktura

Semantyka tego prymitywu przedstawia się następująco:

PHY_AGC.set {*Mode*, *Gain*}.

Parametr trybu *Mode* określa czy warstwa PHY pracuje w trybie automatycznego wzmocnienia czy nie. Może on przyjąć jedną z dwóch wartości:

0: Automatyczny;

1: Ręczny.

Parametr wzmocnienia *Gain* określa początkowe wzmocnienie odbierania w trybie automatycznym. Może on przyjąć jedną z wartości N:

0: *min_gain* dB;

528 1: $\text{min_gain} + \text{step}$ dB;

529 2: $\text{min_gain} + 2 * \text{step}$ dB;

530 ...

531 N-1: $\text{min_gain} + (N-1) * \text{step}$ dB.

532 gdzie min_gain i N zależą od konkretnej implementacji. Wartość step również jest kwestią implementacji,
533 ale nie powinna wynosić więcej niż 6 dB. Maksymalna wartość wzmocnienia $\text{Gain min_gain} + (N-1) * \text{step}$
534 powinna wynosić co najmniej 21 dB.

535 3.10.3.2.3 Użycie

536 Prymityw generowany jest przez warstwę MAC, gdy tryb wzmocnienia odbierania ma zostać zmieniony.

537 3.10.3.3 PHY_AGC.get

538 3.10.3.3.1 Funkcja

539 Prymityw PHY_AGC.get jest przekazywany do jednostki warstwy PHY przez warstwę MAC w celu uzyskania
540 trybu automatycznego wzmocnienia warstwy PHY.

541 3.10.3.3.2 Struktura

542 Semantyka tego prymitywu przedstawia się następująco:

543 PHY_AGC.get{ }.

544 3.10.3.3.3 Użycie

545 Prymityw generowany jest przez warstwę MAC, gdy musi ona znać tryb wzmocnienia odbierania, który
546 został skonfigurowany.

547 3.10.3.4 PHY_AGC.confirm

548 3.10.3.4.1 Funkcja

549 Prymityw PHY_AGC.confirm jest przekazywany do jednostki warstwy PHY przez warstwę MAC w celu
550 odpowiedzi na polecenie PHY_AGC.set lub PHY_AGC.get.

551 3.10.3.4.2 Struktura

552 Semantyka tego prymitywu przedstawia się następująco:

553 PHY_AGC.confirm {*Mode*, *Gain*}.

554 Parametr trybu *Mode* określa czy warstwa PHY jest skonfigurowana do pracy w trybie automatycznego
555 wzmocnienia czy nie. Może on przyjąć jedną z dwóch wartości:

556 0: Automatyczny;

557 1: Ręczny.

558 Parametr wzmocnienia *Gain* określa bieżące wzmocnienie odbierania. Może on przyjąć jedną z wartości N:

559 0: *min_gain* dB;

560 1: *min_gain* + *step* dB;

561 2: *min_gain* + 2**step* dB;

562 ...

563 N-1: *min_gain* + (N-1)**step* dB.

564 gdzie *min_gain* i N zależą od konkretnej implementacji. Wartość *step* również jest kwestią implementacji,
565 ale nie powinna wynosić więcej niż 6 dB. Maksymalna wartość wzmocnienia *Gain* *min_gain* + (N-1)**step*
566 powinna wynosić co najmniej 21 dB.

567 3.10.3.5 PHY_Timer.get

568 3.10.3.5.1 Funkcja

569 Prymityw PHY_TIMER.get jest przekazywany do jednostki warstwy PHY przez warstwę MAC w celu
570 uzyskania czasu, w którym rozpoczęta ma zostać transmisja.

571 3.10.3.5.2 Struktura

572 Semantyka tego prymitywu przedstawia się następująco:

573 PHY_Timer.get {}.

574 3.10.3.5.3 Użycie

575 Prymityw generowany jest przez warstwę MAC, gdy musi ona znać czas rozpoczęcia transmisji.

576 3.10.3.6 PHY_Timer.confirm

577 3.10.3.6.1 Funkcja

578 Prymityw PHY_TIMER.confirm jest przekazywany do jednostki warstwy MAC przez warstwę PHY w celu
579 odpowiedzi na polecenie PHY_Timer.get.

580 3.10.3.6.2 Struktura

581 Semantyka tego prymitywu przedstawia się następująco:

582 PHY_Timer.confirm {*Time*}.

583 Parametr czasu *Time* określony jest w dziesiątkach mikrosekund. Może on przyjąć wartości pomiędzy 0 a
584 2^{20} -1.

585 3.10.3.7 PHY_CD.get**586 3.10.3.7.1 Funkcja**

587 Prymityw PHY_CD.get jest przekazywany do jednostki warstwy PHY przez warstwę MAC w celu wyszukania
588 sygnału wykrycia nośnej. Algorytm wykrywania nośnej powinien opierać się na wykrywaniu preambuły i
589 rozpoznaniu nagłówka (patrz Punkt 3.4).

590 3.10.3.7.2 Struktura

591 Semantyka tego prymitywu przedstawia się następująco:

592 PHY_CD.get {}.

593 3.10.3.7.3 Użycie

594 Prymityw generowany jest przez warstwę MAC, gdy musi ona wiedzieć czy medium fizyczne jest dostępne.

595 3.10.3.8 PHY_CD.confirm**596 3.10.3.8.1 Funkcja**

597 Prymityw PHY_CD.confirm jest przekazywany do jednostki warstwy MAC przez warstwę PHY w celu
598 odpowiedzi na polecenie PHY_CD.get.

599 3.10.3.8.2 Struktura

600 Semantyka tego prymitywu przedstawia się następująco:

601 PHY_CD.confirm {*cd*, *rsst*, *Time*, *Header*}.

602 Parametr *cd* może przyjąć jedną z dwóch wartości:

603 0: nie wykryto nośnej;

604 1: wykryto nośną.

605 Parametr *rsst* to wskazanie siły odebranego sygnału i odnosi się do preambuły. Ma on znaczenie jedynie,
606 gdy *cd* = 1. Może on przyjąć jedną z szesnastu wartości:

607 0: ≤ 70 dBuV;

608 1: ≤ 72 dBuV;

609 2: ≤ 74 dBuV;

610 ...

611 15: > 98 dBuV.

612 Parametr *Time* wskazuje moment, w którym bieżąca jednostka danych PPDU zakończy się. Ma on znaczenie
613 jedynie, gdy *cd* = 1. Gdy *cd* równa się 0, parametr *Time* przyjmie wartość 0. Jeśli *cd* równa się 1, ale czas
614 trwania całej PPDU jest dalej nieznanym (tj. nagłówek nie został jeszcze przetworzony), parametr *header*
615 przyjmie wartość 1, a parametr *Time* wskaże moment, w którym przetwarzanie nagłówka się zakończy,

określony w dziesiątkach mikrosekund. W każdym innym przypadku wartość parametru *Time* wskazuje moment, w którym bieżąca jednostka danych PPDU zakończy się i jest on określony w dziesiątkach mikrosekund. Parametr *Time* odnosi się do punktu bezwzględnego w czasie, więc nazywany jest zegarem systemowym.

Parametr nagłówek *header* może przyjąć jedną z dwóch wartości:

1: jeśli wykryto preambułę, ale czas trwania całej jednostki PPDU nie jest jeszcze znany na podstawie dekodowania nagłówka;

0: w każdym innym przypadku.

3.10.3.9 PHY_NL.get

3.10.3.9.1 Funkcja

Prymityw PHY_NL.get jest przekazywany do jednostki warstwy PHY przez warstwę MAC w celu uzyskania zaokrąglonej wartości szumu.

3.10.3.9.2 Struktura

Semantyka tego prymitywu przedstawia się następująco:

PHY_NL.get {}.

3.10.3.9.3 Użycie

Prymityw generowany jest przez warstwę MAC, gdy musi ona znać poziom szumu obecny w linii energetycznej.

3.10.3.10 PHY_NL.confirm

3.10.3.10.1 Funkcja

Prymityw PHY_NL.confirm jest przekazywany do jednostki warstwy MAC przez warstwę PHY w celu odpowiedzenia na polecenie PHY_NL.get.

3.10.3.10.2 Struktura

Semantyka tego prymitywu przedstawia się następująco:

PHY_NL.confirm {*noise*}.

Parametr szumu *noise* może przyjąć jedną z szesnastu wartości:

0: ≤ 50 dBuV;

1: ≤ 53 dBuV;

2: ≤ 56 dBuV;

...

15: > 92 dBuV.

647 3.10.3.11 PHY_SNR.get**648 3.10.3.11.1 Funkcja**

649 Prymityw PHY_SNR.get jest przekazywany do jednostki warstwy PHY przez warstwę MAC w celu uzyskania
650 wartości stosunku sygnału do szumu, określanej jako stosunek mierzonego poziomu sygnału odebranego
651 do poziomu szumu ostatniej odebranej jednostki PPDU. Obliczenia stosunku sygnału do szumu (SNR)
652 opisano w Załącznik B.

653 3.10.3.11.2 Struktura

654 Semantyka tego prymitywu przedstawia się następująco:

655 PHY_SNR.get {}.

656 3.10.3.11.3 Użycie

657 Prymityw generowany jest przez warstwę MAC, gdy musi ona znać stosunek sygnału do szumu w celu
658 przeanalizowania charakterystyk kanału i wywołania procedur zarządzania stabilnością.

659 3.10.3.12 PHY_SNR.confirm**660 3.10.3.12.1 Funkcja**

661 Prymityw PHY_SNR.confirm jest przekazywany do jednostki warstwy MAC przez warstwę PHY w celu
662 odpowiedzenia na polecenie PHY_SNR.get.

663 3.10.3.12.2 Struktura

664 Semantyka tego prymitywu przedstawia się następująco:

665 PHY_SNR.confirm{SNR}.

666 Parametr SNR odnosi się do stosunku sygnału do szumu, określanego jako stosunek mierzonego poziomu
667 sygnału odebranego do poziomu szumu ostatniej odebranej jednostki PPDU. Może on przyjąć jedną z ośmiu
668 wartości. Mapowanie 3-bitowego indeksu do rzeczywistej wartości SNR, zgodnie z obliczeniami w
669 Załącznik B podano poniżej:

670 0: ≤ 0 dB;

671 1: ≤ 3 dB;

672 2: ≤ 6 dB;

673 ...

674 7: > 18 dB.

675 3.10.3.13 PHY_ZCT.get**676 3.10.3.13.1 Funkcja**

677 Prymityw PHY_ZCT.get jest przekazywany do jednostki warstwy PHY przez warstwę MAC w celu uzyskania
678 czasu zera napięcia sieci pomiędzy ostatnią transmisją lub odbiorem, a przejściem przez zero sieci.

679 3.10.3.13.2 Struktura

680 Semantyka tego prymitywu przedstawia się następująco:

681 PHY_ZCT.get {}.

682 3.10.3.13.3 Użycie

683 Prymityw generowany jest przez warstwę MAC, gdy musi ona znać czas przejścia przez zero sieci, np. w celu
684 obliczenia fazy, do której podłączony jest węzeł.

685 3.10.3.14 PHY_ZCT.confirm

686 3.10.3.14.1 Funkcja

687 Prymityw PHY_ZCT.confirm jest przekazywany do jednostki warstwy MAC przez warstwę PHY w celu
688 odpowiedzi na polecenie PHY_ZCT.get.

689 3.10.3.14.2 Struktura

690 Semantyka tego prymitywu przedstawia się następująco:

691 PHY_ZCT.confirm {Time}.

692 Parametr *Time* to chwila w czasie, w której miejsce miało ostatnie zdarzenie przejścia przez zero.

693 3.10.4 Prymitywy zarządzania PHY

694 3.10.4.1 Ogólne

695 Prymitywy zarządzania warstwą PHY umożliwiają jednostce zarządzającej warstwą PHY łączenie się z
696 jednostkami zarządzającymi górną warstwą. Realizacja tych prymitywów jest opcjonalna. Patrz Rys. 17, aby
697 zobaczyć ogólną strukturę prymitywów zarządzania warstwy PHY.

698
699 Tabela 5 - Prymitywy zarządzania warstwą fizyczną

Prymityw	set (ustaw)	get (uzyskaj)	confirm (zatwierdź)
PLME_RESET	X		X
PLME_SLEEP	X		X
PLME_RESUME	X		X
PLME_TESTMODE	X		X
PLME_GET		X	X

701 3.10.4.2 PLME_RESET.request

702 3.10.4.2.1 Funkcja

703 Prymityw PLME_RESET.request wywoływany jest w celu żądania od warstwy PHY zresetowania bieżącego
704 stanu funkcjonalnego. W wyniku tej prymitywy warstwa PHY powinna wyzerować wszystkie stany
705 wewnętrzne i opróżnić wszystkie bufor, aby usunąć wszystkie zakolejkowane dane odbierania lub

wysyłania. Wszystkie prymitywy SET wywoływane są przez PLME i adresowane do PHY w celu ustawienia parametrów w PHY. Prymityw GET jest również wywoływany przez PLME, ale jest stosowany wyłącznie do odczytu parametrów PHY

709 **3.10.4.2.2 Struktura**

710 Semantyka tego prymitywu przedstawia się następująco:

711 PLME_RESET.request{}

712 **3.10.4.2.3 Użycie**

713 Jednostki zarządzające górną warstwą wywołają ten parametr w celu rozwiązania wszystkich
714 nieprawidłowości na poziomie systemu, które wymagają przerywania wszystkich zakolejkowanych
715 transmisji i ponownego uruchomienia wszystkich działań od stanu inicjalizacji.

716 **3.10.4.3 PLME_RESET.confirm**

717 **3.10.4.3.1 Funkcja**

718 Prymityw PLME_RESET.confirm generowany jest w odpowiedzi na prymityw PLME_RESET.request.
719 Zapewnia on wskazanie czy żądane resetowanie zostało przeprowadzone z powodzeniem czy nie.

720 **3.10.4.3.2 Struktura**

721 Semantyka tego prymitywu przedstawia się następująco:

722 PLME_RESET.confirm{*Result*}.

723 Parametr *Result* przyjmuje jedną z następujących wartości:

724 0: Powodzenie;

725 1: Niepowodzenie. Błąd resetowania z przyczyn wdrożeń wewnętrznych.

726 **3.10.4.3.3 Użycie**

727 Prymityw jest generowany w odpowiedzi na PLME_RESET.request.

728 **3.10.4.4 PLME_SLEEP.request**

729 **3.10.4.4.1 Funkcja**

730 Prymityw PLME_SLEEP.request wywoływany jest w celu żądania od warstwy PHY wstrzymania działań, w
731 tym wszystkich działań odbiorczych. Warstwa PHY powinna ukończyć wszystkie oczekujące transmisje przed
732 przejściem w tryb uśpienia.

733 **3.10.4.4.2 Struktura**

734 Semantyka tego prymitywu przedstawia się następująco:

735 PLME_SLEEP.request{}

736 3.10.4.4.3 Użycie

737 Mimo że specyfikacja odnosi się do komunikacji przez linie energetyczne, wciąż może być przedmiotem
738 innych aplikacji w celu optymalizacji zużycia energii. Prymityw ten ma na celu pomóc tym aplikacjom
739 osiągnąć ten cel.

740 3.10.4.5 PLME_SLEEP.confirm**741 3.10.4.5.1 Funkcja**

742 Prymityw PLME_SLEEP generowany jest w odpowiedzi na prymityw PLME_SLEEP.request i zapewnia
743 informacje czy żądany stan uśpienia został skutecznie wprowadzony czy nie.

744 3.10.4.5.2 Struktura

745 Semantyka tego prymitywu przedstawia się następująco:

746 PLME_SLEEP.confirm{*Result*}.

747 Parametr *Result* przyjmuje jedną z następujących wartości:

748 0: Powodzenie;

749 1: Niepowodzenie. Żądane wprowadzenie w stan uśpienia nie powiodło się z przyczyn wdrożeń
750 wewnętrznych;

751 2: Warstwa PHY znajduje się już w trybie uśpienia.

752 3.10.4.5.3 Użycie

753 Prymityw jest generowany w odpowiedzi na PLME_SLEEP.request

754 3.10.4.6 PLME_RESUME.request**755 3.10.4.6.1 Funkcja**

756 Prymityw PLME_RESUME.request wywoływany jest w celu żądania od warstwy PHY wznowienia
757 wstrzymanych działań. W wyniku tego prymitywu warstwa PHY rozpoczyna normalną transmisję i funkcje
758 odbiorcze.

759 3.10.4.6.2 Struktura

760 Semantyka tego prymitywu przedstawia się następująco:

761 PLME_RESUME.request{}

762 3.10.4.6.3 Użycie

763 Prymityw ten wywoływany jest przez jednostki zarządzające górną warstwą w celu wznowienia normalnych
764 działań warstwy PHY, zakładając że warstwa PHY znajduje się aktualnie w stanie wstrzymania, jako wynik
765 poprzedniego prymitywu PLME_SLEEP.request.

766 **3.10.4.7 PLME_RESUME.confirm**

767 **3.10.4.7.1 Funkcja**

768 Prymityw PLME_RESUME.confirm generowany jest w odpowiedzi na prymityw PLME_RESUME.request i
769 podaje informacje na temat statusu żadanego wznowienia pracy.

770 **3.10.4.7.2 Struktura**

771 Semantyka tego prymitywu przedstawia się następująco:

772 PLME_RESUME.confirm{*Result*}.

773 Parametr *Result* przyjmuje jedną z następujących wartości:

774 0: Powodzenie;

775 1: Niepowodzenie. Żądane wznowienie pracy nie powiodło się z przyczyn wdrożeń wewnętrznych;

776 2: Warstwa PHY jest już w pełni funkcjonalna.

777 **3.10.4.7.3 Użycie**

778 Prymityw jest generowany w odpowiedzi na PLME_RESUME.request.

779 **3.10.4.8 PLME_TESTMODE.request**

780 **3.10.4.8.1 Funkcja**

781 Prymityw PLME_TESTMODE jest wywoływany w celu wprowadzenia warstwy fizycznej PHY w tryb testowy
782 (określony przez parametr trybu *Mode*). Jako parametr wejściowy stosowany jest określony tryb
783 funkcjonalny wybierany spośród różnych możliwych trybów. Po otrzymaniu tego prymitywu warstwa PHY
784 powinna ukończyć wszystkie oczekujące w buforze transmisje przed przejściem w tryb testowy.

785 **3.10.4.8.2 Struktura**

786 Semantyka tego prymitywu przedstawia się następująco:

787 PLME_TESTMODE.request{*enable, mode, modulation, pwr_level*}.

788 Parametr *enable* uruchamia lub zatrzymuje tryb testowy i może przyjąć jedną z dwóch wartości:

789 0: zatrzymanie trybu testowego i powrót do normalnego stanu działania;

790 1: przejście z obecnego stanu działania do trybu testowego.

791 Parametr trybu *Mode* wymienia konkretne funkcjonalne zachowania przejawiane, podczas gdy warstwa
792 PHY jest w trybie testowym. Parametr może przyjąć dowolną z dwóch wartości:

793 0: ciągła transmisja;

794 1: transmisja z 50% cyklem pracy.

795 Parametr modulacji *Modulation* określa, który schemat modulacji stosowany jest podczas transmisji. Może
796 on przyjąć jedną z następujących 8 wartości:

797 0: DBPSK;

798 1: DQPSK;

799 2: D8PSK;

800 3: Nieużywana;

801 4: DBPSK + kod splotowy;

802 5: DQPSK + kod splotowy;

803 6: D8PSK + kod splotowy;

804 7: Nieużywana.

805 Parametr *pwr_level* określa względny poziom, przy którym transmitowany jest sygnał testowy. Może on
806 przyjąć jedną z następujących wartości:

807 0: Maksymalny poziom wyjściowy (MOL);

808 1: MOL -3 dB;

809 2: MOL -6 dB;

810 ...

811 7: MOL -21 dB;

812 **3.10.4.8.3 Użycie**

813 Ten prymityw wywoływany jest przez jednostkę zarządzającą, gdy wymagane są do przeprowadzenia
814 określone testy.

815 **3.10.4.9 PLME_TESTMODE.confirm**

816 **3.10.4.9.1 Funkcja**

817 Prymityw PLME_TESTMODE.confirm generowany jest w odpowiedzi na odpowiedni prymityw
818 PLME_TESTMODE.request w celu wskazania czy przejście na tryb testowy powiodło się czy nie.

819 **3.10.4.9.2 Struktura**

820 Semantyka tego prymitywu przedstawia się następująco:

821 PLME_TESTMODE.confirm{*Result*}.

822 Parametr *Result* przyjmuje jedną z następujących wartości:

823 0: Powodzenie;

824 1: Niepowodzenie. Przejście na tryb testowy nie powiodło się z przyczyn wdrożeń wewnętrznych;

825 2: Warstwa PHY już jest w trybie testowym Testmode.

826 3.10.4.9.3 Użycie

827 Prymityw jest generowany w odpowiedzi na PLME_TESTMODE.request.

828 3.10.4.10 PLME_GET.request

829 3.10.4.10.1 Funkcja

830 Prymityw PLME_GET.request wysyła zapytania dotyczące danego atrybutu PIB.

831 3.10.4.10.2 Struktura

832 Semantyka tego prymitywu przedstawia się następująco:

833 PLME_GET.request{PIBAttribute}

834 Parametr *PIBAttribute* określa konkretne atrybuty wymienione w tabeli w pozycji *Id* , które wyliczają
835 atrybuty PIB (Punkt 6.2.2).

836 3.10.4.10.3 Użycie

837 Prymityw ten wywoływany jest przez jednostkę zarządzającą w celu wysłania zapytania dotyczącego
838 dostępnych atrybutów PIB.

839 3.10.4.11 PLME_GET.confirm

840 3.10.4.11.1 Funkcja

841 Prymityw PLME_GET.confirm generowany jest w odpowiedzi na prymityw PLME_GET.request.

842 3.10.4.11.2 Struktura

843 Semantyka tego prymitywu przedstawia się następująco:

844 PLME_GET.confirm{status, PIBAttribute, PIBAttributeValue}

845 Parametr *status* podaje wynik żądanych informacji i może przyjąć jedną z wartości podanych w Tabeli 6.

846 Tabela 6 – Wartości parametru statusu w prymitywie PLME_GET.confirm

Result (Wynik)	Opis
<i>Done</i> = 0	Wczytanie parametru powiodło się
<i>Failed</i> =1	Błąd wczytywania parametru z przyczyn wdrożeń wewnętrznych.
<i>BadAttr</i> =2	Określony atrybut <i>PIBAttribute</i> nie jest obsługiwany

847

848 Parametr *PIBAttribute* określa konkretne atrybuty wymienione w tabeli w pozycji *Id* , które wyliczają
849 atrybuty PIB (Punkt 6.2.2).

850 Parametr wartości *PIBAttributeValue* określa wartość związaną z danym atrybutem *PIBAttribute*.

851 **3.10.4.11.3 Użycie**

852 Prymityw ten jest generowany w odpowiedzi na prymityw PLME_GET.request.

4 Warstwa Mac

4.1 Omówienie

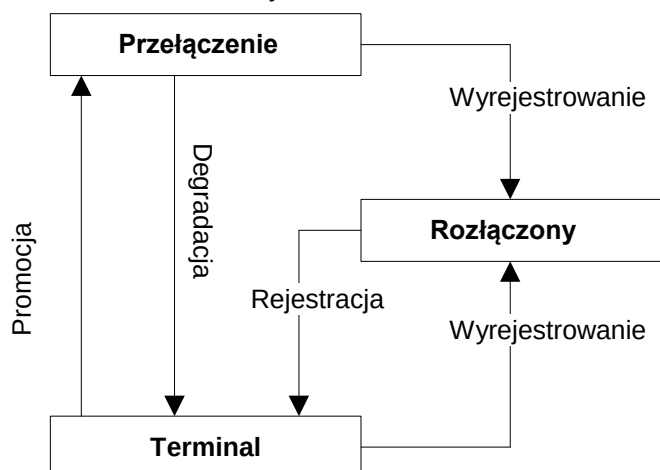
Podsieć może być logicznie postrzegana jako struktura drzewiasta z dwoma rodzajami węzłów: Węzłem podstawowym i węzłami serwisowymi.

- **Węzeł podstawowy:** Znajduje się on u podstaw struktury drzewiastej i działa jako główny węzeł zapewniający łączność wszystkim elementom podsieci. Zarządza on zasobami i połączeniami podsieci. W podsieci jest tylko jeden węzeł podstawowy. Węzeł podstawowy jest początkowo samą podsiecią, a wszystkie inne węzły powinny postępować zgodnie z procesem rejestracji w podsieci.
- **Węzeł serwisowy:** Są to albo liście albo gałęzie w strukturze drzewiastej. Początkowo są one odłączone i postępują zgodnie z procesem rejestracji podanym w punkcie 4.6.1, aby stać się częścią podsieci. Węzły serwisowe pełnią w podsieci dwie funkcje: utrzymywanie łączności z podsiecią dla swoich warstw aplikacji i przełączanie danych innych węzłów w celu propagowania łączności.

Elementy urządzeń, które przejawiają funkcjonalność węzła podstawowego robią to tak długo, jak długo nie są one dokładnie skonfigurowane przez mechanizmy wykraczające poza zakres niniejszej specyfikacji. Z drugiej strony węzeł serwisowy zmienia swoje zachowanie dynamicznie z funkcji „Terminala” do „Przełączenia” lub w drugim kierunku. Zmiany stanów funkcjonalnych występują w odpowiedzi na określone wcześniej zdefiniowane zdarzenia w sieci. Rys. 18 pokazuje diagram stanów funkcjonalnych węzła serwisowego.

Trzy stany funkcjonalne węzła serwisowego to: **Rozłączony**, **Terminal** i **Przełączenie**:

- **Rozłączony:** Jest to początkowy stan funkcjonalny węzłów serwisowych. Jeśli węzeł serwisowy jest Rozłączony, nie może on przesyłać danych, ani przełączać danych innych węzłów. Jego główną funkcją jest szukanie podsieci w swoim zasięgu i spróbowanie rejestracji w niej.
- **Terminal:** W tym stanie funkcjonalnym węzeł serwisowy jest w stanie nawiązać połączenia i przesyłać dane, ale nie może przełączać danych innych węzłów.
- **Przełączenie:** W tym stanie funkcjonalnym węzeł serwisowy jest w stanie wykonywać funkcje terminala. Dodatkowo może on przesyłać dane do i z innych węzłów w tej samej podsieci. Jest to punkt odgałęzienia na strukturze drzewiastej.



Rys. 18 - Stany węzła serwisowego

882 Zdarzenia i powiązane procesy uruchamiające zmiany z jednego stanu funkcjonalnego na drugi to:

- 883 • **Rejestrowanie:** proces, w którym węzeł serwisowy umieszcza się na liście węzłów zarejestrowanych
884 w węźle podstawowym. Skuteczne zakończenie tego procesu oznacza, że węzeł serwisowy jest
885 częścią podsieci. Tak więc stanowi on przejście między stanem Rozłączenia a stanem Terminal.
- 886 • **Wyrejestrowanie:** proces, w którym węzeł serwisowy usuwa się z listy węzłów zarejestrowanych w
887 węźle podstawowym. Wyrejestrowanie może być inicjowane przez Węzeł serwisowy lub węzeł
888 podstawowy. Węzeł serwisowy może wyrejestrować się, aby znaleźć lepszy punkt zaczepienia, tj.
889 zmienić węzeł przełączający, przez który dołączony jest on do sieci. Węzeł podstawowy może
890 wyrejestrować zarejestrowany węzeł serwisowy w wyniku niepowodzenia procedur MAC.
891 Skuteczne zakończenie tego procesu oznacza, że węzeł serwisowy jest Rozłączony i nie jest już
892 częścią podsieci.
- 893 • **Promocja:** proces, w którym węzeł serwisowy jest zakwalifikowany do przełączenia (powtórzenie,
894 przesłanie dalej) ruchu danych z innych węzłów i działania jako gałąź w strukturze drzewiastej
895 podsieci. Skuteczna promocja stanowi przejście pomiędzy terminalem a przełączeniem. Gdy węzeł
896 serwisowy jest Rozłączony, nie może on bezpośrednio przechodzić do stanu Przełączenie.
- 897 • **Degradacja:** proces, w którym węzeł serwisowy przestaje być gałęzią w strukturze drzewiastej
898 podsieci. Skuteczna degradacja stanowi przejście pomiędzy przełączeniem a terminalem.

899 4.2 Adresowanie

900 4.2.1 Ogólne

901 Każdy węzeł posiada 48-bitowy uniwersalny adres MAC określony w normie IEEE 802:2001 i nazywany EUI-
902 48. Każdy EUI-48 jest przypisywany w czasie procesu produkcyjnego i jest stosowany do identyfikacji węzła
903 w czasie procesu rejestracji.

904 EUI-48 węzła podstawowego w unikalny sposób identyfikuje swoją podsieć. EUI-48 nazywany jest adresem
905 podsieci (SNA).

906 Identyfikator przełączenia lokalnego (LSID) jest unikalnym 8-bitowym identyfikatorem dla każdego węzła
907 przełączającego wewnątrz podsieci. Węzeł podstawowy podsieci przypisuje LSID podczas procesu promocji.
908 Węzeł przełączający jest uniwersalnie identyfikowany przez SNA lub LSID. LSID = 0x00 jest zastrzeżony dla
909 węzła podstawowego. LSID = 0xFF jest zarezerwowany, by oznaczać w określonych polach „nieprzypisany”
910 lub „nieprawidłowy” (patrz Tabela 19).). To szczególne użycie wartości 0xFF jest zawsze wyraźnie
911 zaznaczone przy opisie tych pól i nie powinno być stosowane w innych polach.

912 Podczas procesu rejestracji, każdy węzeł serwisowy otrzymuje 14-bitowy identyfikator węzła lokalnego
913 (LNID). LNID identyfikuje pojedynczy węzeł serwisowy spośród węzłów serwisowych, które bezpośrednio
914 zależą od danego przełączenia. Połączenie LNID i SID węzła serwisowego (bezpośredniego LSID
915 przełączenia) tworzy 22-bitowy identyfikator węzła (NID). NID identyfikuje pojedynczy węzeł serwisowy w
916 danej podsieci. LNID = 0x0000 nie można przypisać do Terminala, ponieważ odnosi się on do jego
917 przełączenia bezpośredniego. LNID = 0x3FFF jest zarezerwowany dla ruchu broadcast i multicast (patrz
918 punkt 4.2.3, aby uzyskać więcej informacji). W określonych polach LNID = 0x3FFF może być również użyty
919 jako „nieprzypisany” lub „nieprawidłowy” (patrz Tabela 7 i Tabela 15). To szczególne użycie wartości 0x3FFF

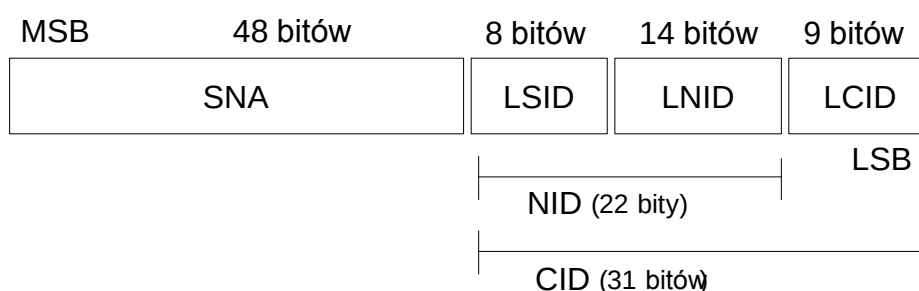
920 jest zawsze wyraźnie zaznaczone przy opisie tych pól i nie powinno być stosowane w ten sposób innych
 921 polach.

922 Podczas nawiązywania połączenia 9-bitowy Identyfikator połączenia lokalnego (LCID) jest rezerwowany.
 923 Identyfikator połączenia lokalnego identyfikuje pojedyncze połączenie w węźle. Połączenie NID i LCID
 924 tworzy 31-bitowy identyfikator połączenia (CID). CID identyfikuje pojedyncze połączenie w danej podsieci.
 925 Wszelkie połączenia są uniwersalnie identyfikowane przez SNA lub LSID. Wartości LCID są przydzielane z
 926 następującymi zasadami:

927 LCID=0x000 do 0x0FF, dla połączeń wymaganych przez węzeł podstawowy. Alokacja powinna być
 928 dokonana przez Węzeł podstawowy.

929 LCID=0x100 do 0x1FF, dla połączeń wymaganych przez węzeł serwisowy. Alokacja powinna być
 930 dokonana przez Węzeł serwisowy.

931 Pełną strukturę adresowania i długości pól pokazano na Rys. 19



932

933

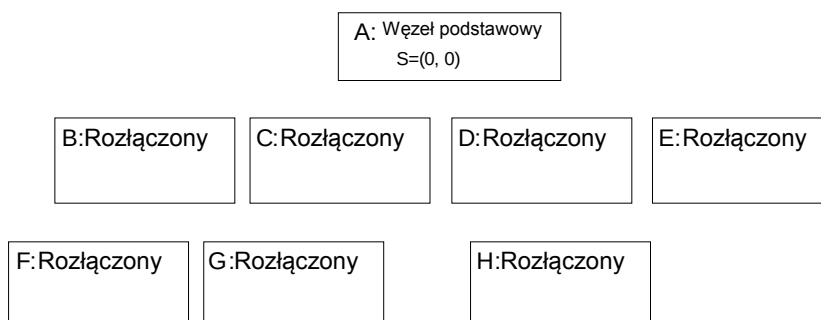
Rys. 19 - Struktura adresowania

934 Gdy węzeł serwisowy w stanie *Terminal* rozpoczyna proces promocji, węzeł podstawowy przydziela
 935 unikalny identyfikator przełączenia, który stosowany jest przez to urządzenie po przejściu na stan
 936 przełączenia jako SID tego przełączenia. Promowany węzeł serwisowy w dalszym ciągu stosuje ten sam NID,
 937 jakiego używał przed promocją, tj. zachowuje SID z następnego poziomu do adresowania całego
 938 wygenerowanego ruchu do lokalnych procesów aplikacji. Aby zachować rozróżnienie pomiędzy tymi
 939 dwoma identyfikatorami przełączenia, identyfikator przełączenia przypisany do węzła serwisowego w czasie
 940 promocji nazywany jest Identyfikatorem przełączenia lokalnego (LSID). Należy zauważyć, że LSID urządzenia
 941 przełączającego będzie SID urządzeń, które łączą się przez niego z podsiecią.

942 Każdy węzeł serwisowy ma poziom w topologicznej strukturze drzewiastej. Węzły serwisowe, które są
 943 bezpośrednio połączone z węzłem podstawowym mają poziom 0. Poziom dowolnego węzła serwisowego
 944 nie bezpośrednio połączonego z węzłem podstawowym to poziom jego bezpośredniego przełączenia plus
 945 jeden.

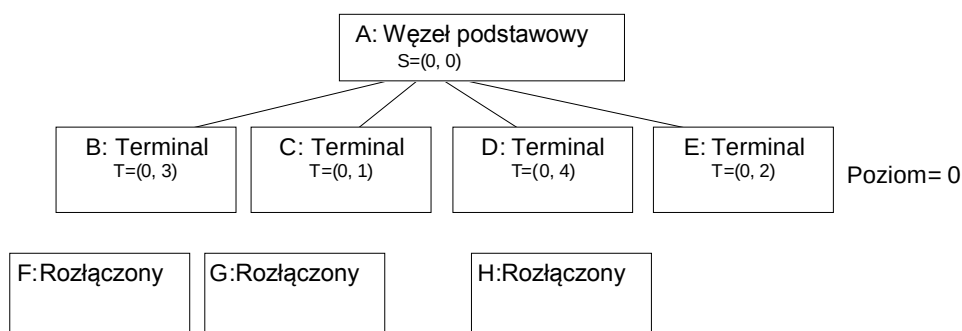
946 4.2.2 Przykład konwersji adresu

947 Rys. 20 pokazuje przykład, w którym odłączone węzły serwisowe próbują zarejestrować się na węźle
 948 podstawowym. W tym przykładzie adresowanie będzie miało następującą nomenklaturę: (SID, LNID).
 949 Początkowo jedyny węzeł z adresem w węźle podstawowym A, który ma NID = (0,0).



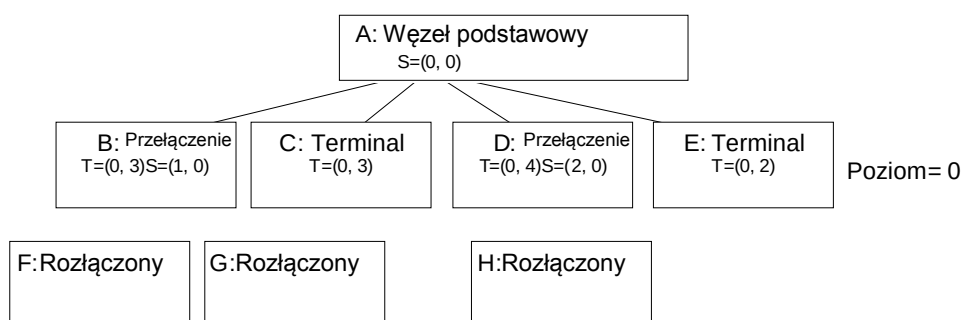
Rys. 20 – Przykład konwersji adresu - faza 1

Każdy inny węzeł podsieci będzie próbował zarejestrować się do węzła podstawowego. Jedynie węzły B, C, D i E są w stanie zarejestrować się w tej podsieci i uzyskać swoje NID. Rys. 21 pokazuje status węzłów po procesie rejestracji. Ponieważ zarejestrowały się one do węzła podstawowego, uzyskują one SID węzła podstawowego i unikalny LNID. Poziom nowo zarejestrowanych węzłów wynosi 0, ponieważ połączone są one bezpośrednio z węzłem podstawowym.



Rys. 21 – Przykład konwersji adresu - faza 2

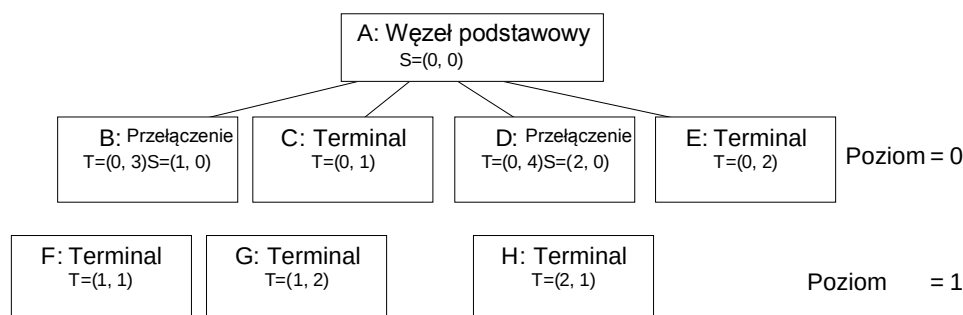
Węzły F, G i H nie mogą łączyć się bezpośrednio z węzłem podstawowym, który jest aktualnie jedynym przełącznikiem w podsieci. F, G i H będą wysyłać żądania PNPDU, które doprowadzą do wysłania przez węzły D i B żądania dla nich promocji w celu rozszerzenia zakresu podsieci. W czasie promocji obu przydzielone zostaną unikalne identyfikatory SID. Rys. 22 pokazuje nowy status sieci po promocji Węzłów B i D. Każdy węzeł przełączniowy będzie nadal korzystać z identyfikatora NID przypisanego do niego w czasie procesu rejestracji dla własnej komunikacji jako węzeł terminala. Nowy identyfikator SID będzie stosowany dla wszystkich funkcji przełączania.



Rys. 22 – Przykład konwersji adresu - faza 3

Po zakończeniu procesu promocji B i D, Węzły F, G i H rozpoczną proces rejestracji i przydzielone zostaną im unikalne LNID. Każdy węzeł podsieci uzyska unikalny NID do komunikacji jak Terminal, a węzły przełączające dostaną unikalne SID do celów przełączania. Poziom nowo zarejestrowanych węzłów wynosi 1 ponieważ

rejestrowane są one w węzłach poziomu 0. Po zakończeniu konwersji topologii i alokacji adresu przykładowa podsieć wyglądać będzie jak na Rys. 23



Rys. 23 – Przykład konwersji adresu - faza 4

4.2.3 Adresowanie broadcast i multicast

Adresy multicast i broadcast stosowane są do przekazywania danych do wielu węzłów. Istnieje kilka typów adresów multicast i broadcast w zależności od kontekstu związanego z przepływem ruchu. Tabela 7 opisuje różne typy adresowania broadcast i multicast oraz skojarzone z nimi pola SID i LNID.

Tabela 7 - Adres broadcast i multicast

Typ	LNID	Opis
Broadcast	0x3FFF	Korzystając z tego adresu jako miejsca docelowego, pakiety powinny dotrzeć do każdego węzła z podsieci.
Multicast	0x3FFE	Ten typ adresu odnosi się do grup multicast. Grupa multicast definiowana jest przez Identyfikator połączenia lokalnego.
Unicast	not 0x3FFF not 0x3FFE	Adres tego typu odnosi się tylko do węzła z podsieci, którego SID i LNID odpowiadają polom adresu.

4.3 Opis funkcjonalny MAC

4.3.1 Uruchomienie węzła podstawowego

Węzeł serwisowy jest początkowo rozłączony. Jedynymi funkcjami, które mogą być wykonywane w stanie funkcjonalnym *Rozłączony* są: odbiór wszelkich sygnałów kanału i wysyłanie PNPDU. Każdy węzeł serwisowy zarządza tablicą przełączania, która jest aktualizowana wraz z odebraniem sygnału z dowolnego nowego węzła przełączającego. Na podstawie lokalnych polityk wdrożeniowych węzeł serwisowy może wybrać węzeł przełączający z tablicy przełączania i kontynuować proces rejestracji z tym węzłem przełączającym. Kryterium wyboru węzła przełączającego z tabeli przełączania leży poza zakresem niniejszej specyfikacji.

Węzeł serwisowy powinien nasłuchiwać kanał przez okres co najmniej *macMinSwitchSearchTime* przed stwierdzeniem, że nie odebrano żadnego sygnału. Ewentualnie może on dodać kilka przypadkowych zmian do *macMinSwitchSearchTime*, ale zmiana ta nie może być większa niż 10 % wartości *macMinSwitchSearchTime*. Jeśli w tym czasie nie zostaną odebrane żadne sygnały, Węzeł serwisowy

993 powinien nadać PNPDU. PNPDU są nadawane przy najbardziej zaawansowanym schemacie modulacji w
994 celu zapewnienia maksymalnego pokrycia. Węzeł serwisowy próbujący promować któryś z węzłów
995 Terminala w pobliżu nie powinien przysyłać więcej niż *macMaxPromotionPdu* PNPDU na
996 *macPromotionPduTxPeriod* jednostek czasu. Węzeł serwisowy powinien również zapewniać, że nadawanie
997 jednostek PNPDU jest losowo rozmieszczone. Pomiędzy kolejnymi emisjami zawsze muszą występować
998 losowe odstępy.

999 Aby nie zalać sieci jednostkami PNPDU, szczególnie w przypadkach, gdy kilka urządzeń zasilanych jest w tym
1000 samym czasie, węzły terminala powinny zredukować współczynnik transmisji PNPDU o współczynnik
1001 odbioru PNPDU z innych źródeł. Na przykład, jeśli węzeł odbiera jeden jedną jednostkę PNPDU, gdy wysyła
1002 własne jednostki PNPDU, powinien on zredukować własne transmisje o nie więcej, niż
1003 *macMaxPromotionPdu/2* na *macPromotionPduTxPeriod* jednostek czasu. Podobnie, jeśli otrzymuje on
1004 PNPDU z dwóch różnych źródeł, powinien on zwolnić szybkość wysyłania do nie więcej niż
1005 *macMaxPromotionPdu/3* na *macPromotionPduTxPeriod* jednostek czasu.

1006 Po wybraniu określonego węzła przełączającego, węzeł serwisowy rozpocznie proces rejestracji poprzez
1007 przesłanie pakietu kontrolnego REG (4.4.5.3) do węzła podstawowego. Węzeł przełączający, przez który
1008 węzeł serwisowy ma zamiar przeprowadzać swoją komunikację, wskazany jest w pakiecie kontrolnym REG.

1009 4.3.2 Uruchamianie i zarządzanie podsieciami

1010 Węzły podstawowe są głównie odpowiedzialne za ustawianie i zarządzanie podsiecią. W celu wykonania tej
1011 ostatniej funkcji węzeł podstawowy powinien przeprowadzać:

- 1012 • **Transmisje sygnału.** Węzeł podstawowy i wszystkie węzły przełączające w podsieci powinny
1013 przysyłać sygnały w stałych odstępach czasu. Węzeł podstawowy powinien zawsze przysyłać
1014 dokładnie jeden sygnał na ramkę. Węzły przełączające powinny transmitować sygnały w
1015 częstotliwości zaleconej przez węzeł podstawowy w czasie ich promocji.
- 1016 • **Promocja i degradacja terminali i przełączeń.** Wszystkie żądania promocji generowane przez węzły
1017 terminali po odebraniu PNPDU są kierowane do węzła podstawowego. Węzeł podstawowy
1018 utrzymuje tablicę węzłów przełączających w podsieci i przydziela unikalny SID do nowych żądań
1019 przychodzących. Po odebraniu wielu żądań promocji węzeł podstawowy może, według własnego
1020 uznania, odrzucić kilka żądań. Podobnie węzeł podstawowy odpowiada za degradację
1021 zarejestrowanych węzłów przełączających. Degradacja może zostać zainicjowana przez węzeł
1022 podstawowy (na podstawie procesu decyzji zależnych od wdrożenia) lub być wymagany przez sam
1023 węzeł przełączający.
- 1024 • **Zarządzanie rejestracją.** Węzeł podstawowy odbiera żądania rejestracji od wszystkich nowych
1025 węzłów próbujących stać się częścią podsieci, którą zarządza. Węzeł podstawowy powinien
1026 przetwarzać każdy wniosek o rejestrację, który otrzymuje i na który odpowiada komunikatem
1027 zatwierdzenia lub odrzucenia. Kiedy węzeł podstawowy zatwierdza rejestrację węzła serwisowego,
1028 powinien on przydzielić unikalny NID do wykorzystania dla wszystkich kolejnych komunikacji w
1029 podsieci. Podobnie węzeł podstawowy odpowiada za wyrejestrowanie wszystkich zarejestrowanych
1030 węzłów serwisowych. Wyrejestrowanie może zostać zainicjowane przez węzeł podstawowy (na
1031 podstawie procesu decyzji zależnych od wdrożenia) lub być wymagane przez sam węzeł serwisowy.
- 1032 • **Ustawienia i zarządzanie połączeniem:** Warstwa MAC określona w niniejszym dokumencie jest
1033 zorientowana na połączenie, co oznacza, że wymiana danych jest zawsze poprzedzona nawiązaniem

połączenia. Węzeł podstawowy jest zawsze wymagana dla wszystkich połączeń w podsieci albo jako punkt końcowy połączenia lub jako facylitator (połączenia bezpośrednie, punkt 4.3.6) połączenia.

- **Arbitraż dostępu do kanału.** Wykorzystanie kanału przez urządzenia spełniające specyfikacje może być kontrolowane i bezkolizyjne w określonych okresach czasu oraz otwarte i kolizyjne w innych. Węzeł podstawowy zaleca, który mechanizm będzie stosowany, w jakim czasie i przez jak długo. Ponadto węzeł podstawowy będzie odpowiedzialny za przypisanie kanału do określonych urządzeń w okresach dostępu bezkolizyjnego.
- **Dystrybucja losowej sekwencji wyprowadzania kluczy szyfrowania.** Podczas korzystania z profilu zabezpieczeń 1 (patrz 4.3.8.1) wszystkie komunikaty kontrolne w specyfikacji MAC będą zaszyfrowane przed wysłaniem. Poza komunikatami kontrolnymi transfery danych mogą być również opcjonalnie szyfrowane. Klucz szyfrowania wyprowadzany jest ze 128-bitowego losowego ciągu. Węzeł podstawowy powinien okresowo generować nowy losowy ciąg i dystrybuować go do całej podsieci, tym samym pomagając utrzymać infrastrukturę zabezpieczeń podsieci.
- **Zarządzanie grupą multicast.** Węzeł podstawowy będzie zarządzać wszystkimi grupami multicast w podsieci. Wymagać będzie to przetwarzania wszystkich wniosków węzłów serwisowych o dołączenie i opuszczenie grupy oraz utworzenia komunikatów nieprzewidzianego dołączenia i opuszczenia grupy przez żądania aplikacji węzła podstawowego.

Dodatkowe informacje dotyczące promocji i procedury połączenia można znaleźć w punktach 4.6.3 i 4.6.6.

4.3.3 Dostęp do kanału

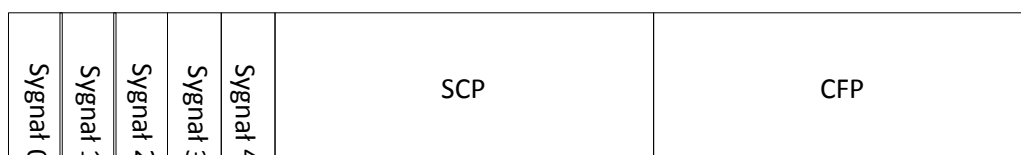
4.3.3.1 Ogólne

Urządzenia w podsieci uzyskują dostęp do kanału na podstawie określonych wytycznych opisanych w niniejszym punkcie. Czas podzielony jest na złożone jednostki abstrakcji do wykorzystania kanałów, zwane Ramkami MAC. Węzły serwisowe i węzeł podstawowy w podsieci mają dostęp do kanału w Okresie współdzielonej kontencji (SCP) lub mogą zażądać dedykowanego Okresu dostępu bezkolizyjnego (CFP).

Dostęp do kanału CFP wymaga od urządzeń żądania alokacji od węzła podstawowego. W zależności od stanu wykorzystania kanału Węzeł podstawowy może przyznać dostęp do żądającego urządzeń na określony czas lub odrzucić żądanie.

Dostęp do kanału SCP nie wymaga arbitrażu. Jednakże urządzenie przesyłające muszą przestrzegać wartości granicznych dla SCP w ramce warstwy MAC. Skład ramki MAC pod kątem SCP i CDP przekazywany jest w każdej ramce jako część sygnału.

Ramka MAC składa się z jednego lub większej liczby sygnałów, jednego Okresu współdzielonej kontencji i zero lub jednego Okresu bezkolizyjnego dostępu (CFP). Jeśli CFP występuje, jego długość wskazywana jest w BPDU.



Rys. 24 – Struktura ramki MAC

1069 4.3.3.2 Sygnał

1070 4.3.3.2.1 Ogólne

1071 BPDU przesyłana jest przez węzeł podstawowy co ($MACFrameLength - MACBeaconLength$) symboli. Węzły
1072 przełączające również przesyłają BPDU w celu zarządzania swoimi częściami podsieci. Przesyłają one BPDU
1073 w regularnych odstępach czasu, ale częstotliwość transmisji nie musi być taka sama, jak częstotliwość węzła
1074 podstawowego, tj. węzeł przełączający może nie wysyłać BPDU w każdej ramce.

1075 Sygnał zawsze ma długość $MACBeaconLength$ symboli. Ta długość to czas trwania sygnału z wyłączeniem
1076 narzutu preambuły warstwy PHY. Ponieważ BPDU odbierane będą przez wszystkie urządzenia w
1077 wyjściowym przełączaniu, wysyłane są one za pomocą najbardziej zaawansowanego schematu modulacji
1078 PHY i kodowania FEC przy maksymalnym poziomie mocy wyjściowej wdrożonym w urządzeniu.
1079 Szczegółowe informacje na temat struktury i treści BPDU podano w punkcie 4.4.4.

1080 Wszystkie węzły serwisowe powinny śledzić sygnały zgodnie z punktem 4.3.4.1.

1081 4.3.3.2.2 Szczeliny sygnału

1082 Pojedyncza ramka może zawierać jednostki BPDU $macBeaconsPerFrame$. Jednostka czasu, w której
1083 przesyłane są BPDU nazywa się szczeliną sygnału. Wszystkie szczeliny sygnału umieszczane są na początku
1084 ramki, tak jak pokazano na Rys. 24 powyżej. Pierwsza szczelina sygnału w każdej ramce zarezerwowana jest
1085 dla węzła podstawowego. Liczba szczelin w ramce może zmieniać się indywidualnie i wskazywana jest przez
1086 węzeł podstawowy w BPDU.

1087 Do węzłów przełączających przypisywana jest szczelina sygnału w czasie ich promocji. Po pakiecie
1088 kontrolnym PRO węzeł podstawowy przesyła pakiet kontrolny BSI, który podaje szczegółowe informacje
1089 określające, która szczelina sygnału zostanie użyta przez nowe urządzenie przełączające.

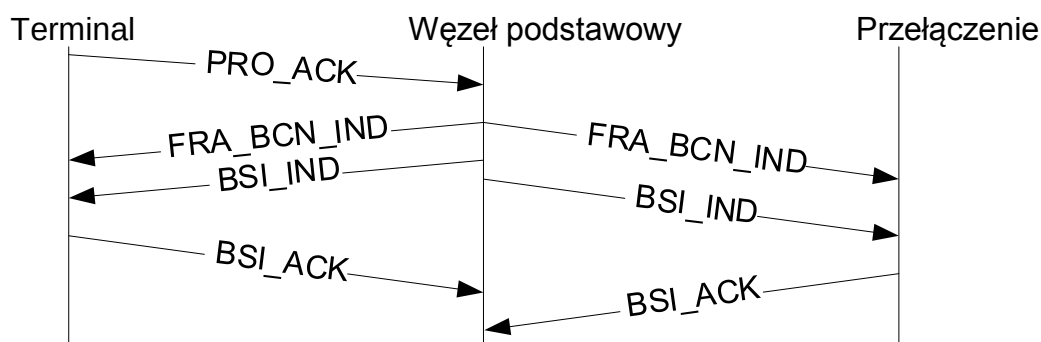
1090 Liczba szczelin sygnału w ramce powinna zostać zwiększona z 1 do co najmniej 2 podczas promocji
1091 pierwszego urządzenia przełączającego w podsieci przez węzeł podstawowy. Podobnie, węzeł podstawowy
1092 nie może zmniejszyć liczby szczelin sygnału w podsieci do 1, gdy w jego podsieci znajduje się węzeł
1093 przełączający.

1094 Wraz z rejestracją każdego nowego przełączenia w podsieci, węzeł podstawowy może zmienić szczelinę
1095 sygnału lub częstotliwość transmisji BPDU (lub oba) już zarejestrowanych urządzeń przełączających. Gdy
1096 taka zmiana nastąpi, węzeł podstawowy przesyła pakiet kontrolny informacji na temat szczeliny sygnału
1097 (BSI) do każdego urządzenia przełączającego, na które ma to wpływ. Urządzenie przełączające adresowane
1098 w pakiecie BSI przesyła zatwierdzenie z powrotem do węzła podstawowego. Urządzenia przełączające
1099 wymagane są do przekazywania pakietów kontrolnych BSI skierowanych do urządzeń przełączających
1100 połączonych przez nie. W czasie reorganizacji szczelin sygnału, jeśli nastąpiła zmiana liczby szczelin na
1101 ramkę, węzeł podstawowy powinien przekazywać pakiet kontrolny FRA (ramkę) do całej podsieci. Pakiet
1102 kontrolny FRA jest wskazaniem zmiany w ogólnej strukturze ramki. W określonych przypadkach może
1103 oznaczać to wzrost w szczelinach Okresu współdzielonej kontencji i zmniejszenie liczby szczelin sygnału.

1104 Urządzenia przełączające, które odbierają pakiet kontrolny FRA powinny przekazywać go do swojej całej
1105 domeny kontrolnej, ponieważ pakiety FRA są informacjami na temat zmian w strukturze ramki.

1106 Jest to wymagane dla całej podsięci, aby uzyskać wspólne zrozumienie struktury ramki, szczególnie w
 1107 rejonach, gdzie urządzenia przełączające wysyłają BPDU w częstotliwościach poniżej jednej jednostki na
 1108 ramkę.

1109 Rys. 25 poniżej pokazuje przykładową sekwencję zmiany szczeliny sygnału dla istniejącego urządzenia
 1110 przełączającego. Powyższy przykład pokazuje zmianę szczeliny sygnału zainicjowaną przez promocję
 1111 urządzenia terminala (PRO_ACK). W tym przypadku po promocji następuje zmiana zarówno w liczbie
 1112 szczelin na ramkę oraz określonych parametrach szczelin już przypisanych do przełączenia.



Rys. 25 – Przykład sekwencjonowania pakietu kontrolnego po promocji

1115 4.3.3.2.3 Zasady alokacji szczeliny sygnału

1116 Zasady alokacji szczeliny sygnału powinny zapewniać, aby w czasie promocji węzeł serwisowy nigdy nie
 1117 otrzymywał pakietu kontrolnego BSI, który zmusza go do przesyłania sygnału w następstwie każdego
 1118 sygnału węzła, w którym jest zarezerwowany.

1119 To zachowanie powinno być zapewnione jeśli informacje BSI są zgodne z jedną lub większą liczbą
 1120 poniższych zasad (BCN oznacza informacje sygnałów węzła serwisowego w którym są zarejestrowane):

- 1121 • BSI.SLT nie jest następstwem BCN.POS;
- 1122 • BSI.SEQ nie jest równa dowolnej BCN.SEQ w superramce;
- 1123 • BSI.FRQ jest większa niż BCN.FRQ.

1124 4.3.3.2.4 Superramka sygnału

1125 Podczas zmiany struktury ramki, dodawania lub usuwania szczeliny sygnału lub zmiany szczeliny sygnału
 1126 przełączenia, niezbędne jest wskazanie, kiedy taka zmiana powinna nastąpić. Wszystkie węzły muszą
 1127 zmieniać się w tym samym czasie. W przeciwnym razie wystąpią kolizje z sygnałami, itd.

1128 Aby rozwiązać ten problem zdefiniowano superramkę. Każdy sygnał zawiera 5-bitową liczbę sekwencji. Tak
 1129 więc 32 ramek tworzy superramkę. Wszystkie komunikaty, które zawierają zmiany w strukturze lub
 1130 wykorzystanie ramki zawierają liczbę sekwencji określającą kiedy powinna nastąpić zmiana. Żądane zmiany
 1131 powinny następować wyłącznie, gdy liczba sekwencji sygnału jest zgodna z liczbą sekwencji w żądaniu
 1132 zmiany.

1133 4.3.3.3 Okres współdzielonej kontencji

1134 4.3.3.3.1 Ogólne

1135 Okres współdzielonej kontencji (SCP) to okres, kiedy dowolne urządzenie w podsieci może przysyłać dane.
1136 SCP rozpoczyna się bezpośrednio po zakończeniu szczeliny sygnału w ramce. Kolizje wynikające z
1137 równoczesnej próby dostępu do kanału unikane są za pomocą mechanizmu CSMA-CA opisanego w tym
1138 punkcie.

1139 Długość okresu SCP może zmieniać się w zależności od ramki i jest wskazywana przez informacje w sygnale.
1140 SCP zawsze ma długość co najmniej *MACMinSCPLength* symboli. Maksymalna dopuszczalna długość SCP w
1141 ramce to (*MACFrameLength* – *MACBeaconLength*) symboli. Maksymalna długość okresu SCP powinna
1142 występować jedynie jeśli nie ma dedykowanych uprawnień dostępu do urządzeń (brak CFP) w podsieci bez
1143 węzłów przełączających (tylko jedna szczelina sygnału).

1144 Stosowanie SCP nie jest ograniczone do ramek, w których odbierane są sygnały. Na niższych poziomach
1145 podsieci, kontrolujący węzeł przełączający może wysyłać sygnały w dużo mniejszych częstotliwościach, niż
1146 raz na ramkę. Dla tych części podsieci struktura ramki będzie w dalszym ciągu taka sama w ramach, w do
1147 których nie przesłano sygnałów. Tym samym węzły serwisowe w tym segmencie mogą nadal korzystać z
1148 SCP według własnego uznania.

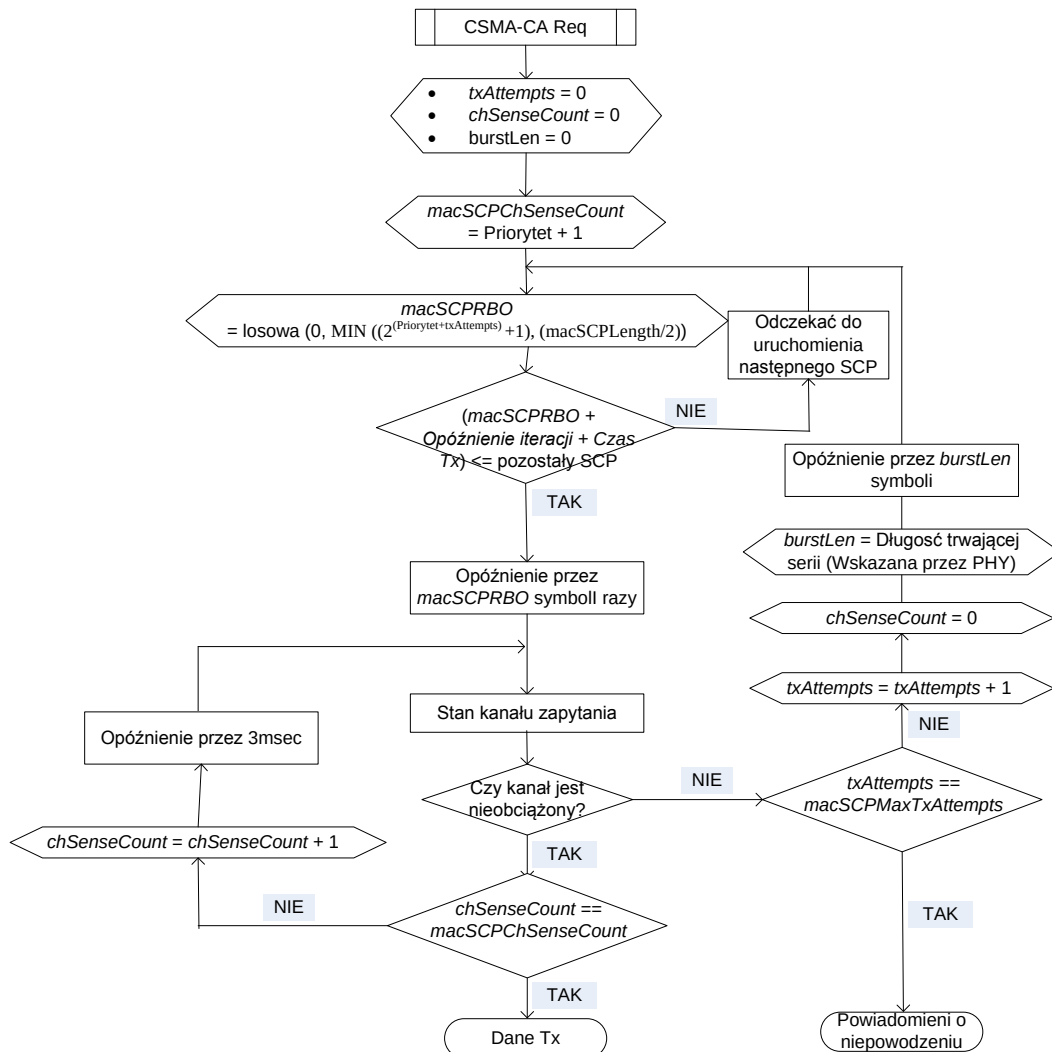
1149 4.3.3.3.2 Algorytm CSMA-CA

1150 Algorytm CSMA-CA wdrożony w urządzeniach działa zgodnie z informacjami pokazanymi na Rys. 26.

1151 Wdrożenia rozpoczynają się od losowego czasu odczekiwania (*macSCPRBO*) opartego na priorytetach
1152 danych kolejgowanych do wysłania. Poziomy priorytetu *MACPriorityLevels* muszą być zdefiniowane w
1153 każdym wdrożeniu, gdzie najniższa wartość wskazuje najwyższy priorytet. W przypadku agregacji danych
1154 priorytet danych masowych zarządzany jest przez zawarte w nim dane o najwyższym prioryecie.
1155 *MacSCPRBO* dla próby transmisji podano poniżej:

1156
$$\text{macSCPRBO} = \text{losowa liczba } (0, \text{MIN} ((2^{(\text{Priorytet} + \text{txAttempts})} + 1), (\text{macSCPLength}/2)))$$

1157 Przed rozpoczęciem czasu odczekiwania urządzenie powinno zapewnić, że pozostały czas SCP jest
1158 wystarczająco długi do dostosowania odczekiwania, liczby iteracji od wykrywania kanału (na podstawie
1159 priorytetów danych) oraz kolejnych transmisji danych. W przeciwnym razie odczekiwanie należy anulować
1160 do czasu rozpoczęcia SCP w kolejnej ramce. Anulowane odczekiwania, które rozpoczynają się w kolejnej
1161 ramce nie powinny przenosić wartości *macSCPRBO* wcześniejszych prób. Wartości *macSCPRBO* powinny
1162 być odnowione po wznowieniu próby transmisji w czasie SCP następnej ramki.



Rys. 26 - Schemat dla algorytmu CSMA-CA

Po zakończeniu czasu symbolu *macSCPRBO* wdrożenia wykonują proces wykrywania kanału. Wykrywanie kanału powinno być przeprowadzane raz lub więcej razy w zależności od priorytetu danych, które mają zostać przesłane. Liczba razy, kiedy wdrożenie musi wykonać proces wykrywania kanału (*macSPChSenseCoun*) jest określana przez priorytet danych do przesłania w następującym stosunku:

$macSCPChSenseCount = Priorytet + 1$

a każde wykrywanie kanału powinno być rozdzielone opóźnieniami 3 ms.

Gdy podczas wykrywania okaże się, że kanał jest beczynny podczas wszystkich okazji *macSCPChSenseCount*, wdrożenie może wywnioskować, że status kanału to *Brak obciążenia* i natychmiast wykonać tę transakcję.

W czasie wszystkich iteracji wykrywania kanału *macSCPChSenseCount*, jeśli wykrywany kanał jest zajęty, wdrożenia powinny zresetować wszystkie zmienne robocze. Lokalny licznik śledzący liczbę razy, gdy kanał jest zajęty powinien być zwiększany o jeden, a proces CSMA-CA powinien uruchomić się ponownie poprzez wygenerowanie nowego *macSCPRBO*. Kolejność pozostałych kroków, począwszy od odczekiwania, powinna być jak wyżej.

1179 Jeśli algorytm CSMA-CA ponownie uruchomi się liczbę razy *macSCPMaTxAttempts* z powodu trwających
1180 transmisji z innych urządzeń w kanale, transmisja powinna zostać anulowana poprzez poinformowanie
1181 górnych warstw o niepowodzeniu CSMA-CA.

1182 4.3.3.3 Pakiety kontrolne MAC

1183 Pakiety kontrolne MAC powinny być przesłane w SCP z priorytetem równym jeden. Odnosi się do
1184 priorytetów w podpunkcie 4.4.2.3

1185 4.3.3.4 Okres bezkolizyjnego dostępu

1186 Każda ramka MAC może opcjonalnie mieć okres bezkolizyjnego dostępu, w którym urządzeniom na
1187 wyraźne żądanie przypisywany jest czas kanału. Jeśli urządzenie w podsieci zażąda bezkolizyjnego okresu
1188 dostępu do kanału, wystąpić może całkowity brak CFP_ALC_REQ_S, a ramka MAC składa się tylko z SCP.
1189 Wszystkie żądania CFP_ALC_REQ_S pochodzące z węzłów terminala lub węzłów przełączających są
1190 adresowane do węzła podstawowego. Pośrednie węzły przełączające wzdłuż ścieżki transmisyjnej działają
1191 wyłącznie na bazie decyzji węzła podstawowego o alokacji. Pojedyncza ramka MAC może zawierać do
1192 *MACCFPMaAlloc* niepokrywających się okresów bezkolizyjnego dostępu.

1193 Węzeł podstawowy może przydzielać nakładające się na siebie czasy w celu zwielokrotnienia węzłów
1194 serwisowych. Takie przydziały mogą prowadzić do potencjalnych zakłóceń. Tym samym węzeł podstawowy
1195 powinien dokonać takich przydziałów jedynie, gdy urządzenia, które stanowią przydzielony dostęp do
1196 kanału dla aktualnego zastosowania są wystarczająco rozdzielone.

1197 Węzeł serwisowy dokonuje żądania alokacji kanału w pakiecie kontrolnym CFP MAC. Węzeł podstawowy
1198 odpowiada na to żądanie poprzez zatwierdzenie lub odrzucenie żądania. W przypadku zatwierdzenia
1199 żądania węzeł podstawowy powinien odpowiedzieć za pomocą lokalizacji czasu alokacji w ramce MAC,
1200 długości czasu alokacji i liczby przyszłych ramek MAC, na podstawie których zostanie ustalony wzór alokacji.
1201 Wzór alokacji obowiązuje do czasu niezapowiedzianej zmiany lokalizacji okresu alokacji z węzła
1202 podstawowego (jako wynik rozpoznania wzoru alokacji kanału) lub wysyłający żądanie węzeł serwisowy
1203 wysyła nieprzewidziane żądanie za pomocą pakietu kontrolnego CFP MAC.

1204 Zmiany wynikające z działań podjętych w komunikacie kontrolnym CFP MAC, które wpływają na ogólną
1205 strukturę ramki MAC wysyłane są do wszystkich urządzeń za pomocą komunikatu kontrolnego MAC FRA.

1206 W podsieci wielopoziomowej, gdy węzeł serwisowy, który nie jest bezpośrednio połączony z węzłem
1207 podstawowym wykonuje żądanie do CFP, węzeł podstawowy powinien przydzielić CFP do wszystkich
1208 pośrednich węzłów serwisowych, tak że cała ścieżka transportu ze źródłowego węzła serwisowego do węzła
1209 podstawowego ma zarezerwowane bezkolizyjne szczeliny czasowe. Węzeł podstawowy powinien przesłać
1210 wiele pakietów kontrolnych CFP. Pierwszym z tych CFP_ALC_IND będzie dla wysyłającego węzła
1211 serwisowego. Wszystkie pozostałe pakiety będą zaadresowane do pośredniego węzła przełączającego.

1212 4.3.4 Śledzenie przełączeń i partnerzy

1213 4.3.4.1 Śledzenie przełączeń

1214 Węzły serwisowe powinny śledzić wszystkie węzły przełączające poprzez zarządzanie listą odebranych
1215 sygnałów. Śledzenie takie powinno informować węzeł na temat jakości odbieranego sygnału z węzłów
1216 przełączających, innych niż te, do których jest podłączony, tym samym umożliwiając zmianę punktów

1217 połączenia (węzeł przełączający) do podsieci jeśli jakość łącza do istniejącego punktu łączności wykracza
1218 poza dopuszczalny poziom.

1219 Należy zauważyć, że zmiana punktu połączenia może być złożona dla węzłów przełączających z powodu
1220 podłączonych do nich urządzeń. Jednakże, w określonych momentach, dynamika sieci może uzasadnić
1221 złożoną reorganizację, a nie kontynuować przy istniejących ograniczonych warunkach.

1222 **4.3.4.2 Śledzenie odłączonych węzłów**

1223 Terminale powinny przetwarzać wszystkie otrzymane jednostki PNPDU. Gdy węzeł serwisowy jest
1224 odłączony, nie ma informacji na temat bieżącej struktury ramki MAC, tak więc PNPDU mogą niekoniecznie
1225 pojawić się w czasie okresu współdzielonej kontencji. Tym samym terminale mogą również śledzić PNPDU
1226 w czasie CFP lub szczelin sygnału.

1227 Podczas przetwarzania odebranego PNPDU węzeł terminala może zdecydować o zignorowaniu go i
1228 niegenerowaniu odpowiednich żądań promocji (PRO_REQ_S). Węzeł terminala powinien zignorować nie
1229 więcej, niż *MACMaxPRNIgnore* PNPDU z tego samego urządzenia. Odbieranie wielu PNPDU z tego samego
1230 urządzenia wskazuje, że w pobliżu rozłączonego węzła nie znajduje się inne urządzenie co oznacza, że nie
1231 będzie możliwości podłączenia tego nowego urządzenia do dowolnej podsieci, jeśli węzeł terminal nie
1232 wnioskuję o promocję dla siebie.

1233 **4.3.5 Przełączanie**

1234 **4.3.5.1 Ogólne**

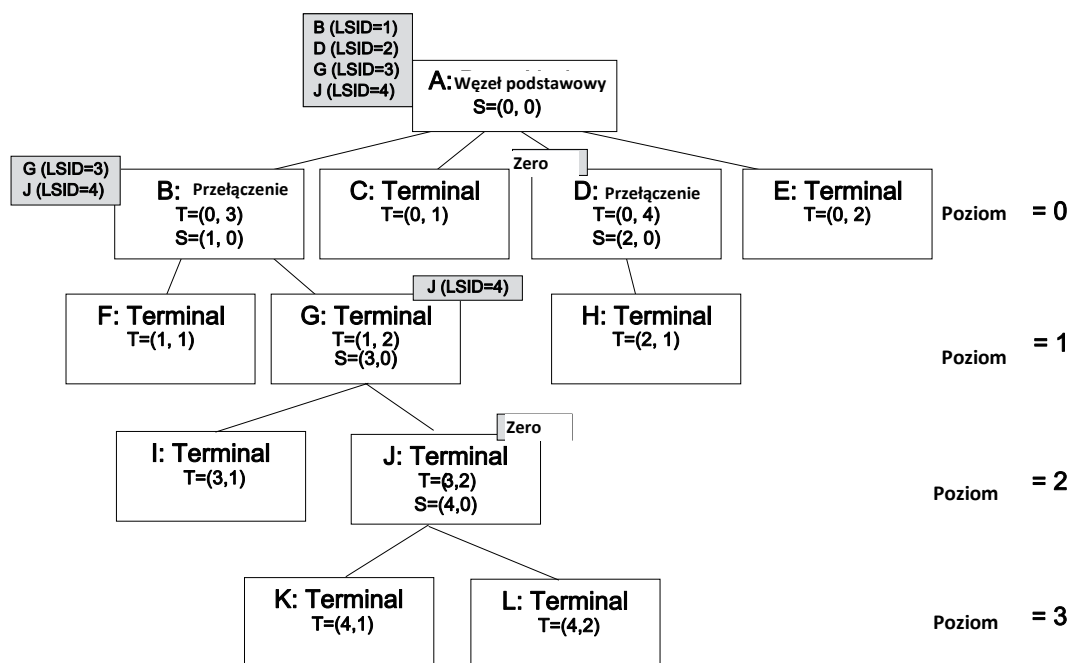
1235 W podsieci węzeł podstawowy nie może komunikować się bezpośrednio z każdym węzłem. Węzły
1236 przełączające przekazują ruch ro/z węzła podstawowego, więc każdy węzeł z podsieci może skutecznie
1237 komunikować się z węzłem podstawowym. Węzły przełączające wybiórczo przekazują ruch, który pochodzi
1238 z lub jest przeznaczony do jednego z węzłów serwisowych w jego hierarchii kontrolnej. Cały inny ruch jest
1239 odrzucany przez przełączenia, tym samym optymalizując przepływ ruchu w sieci.

1240 W tym punkcie stosowane są różne nazwy nagłówka MAC i pakietów. Aby uzyskać informacje na temat ich
1241 pełnej specyfikacji, patrz punkt 4.4.2.

1242 **4.3.5.2 Tablica przełączania**

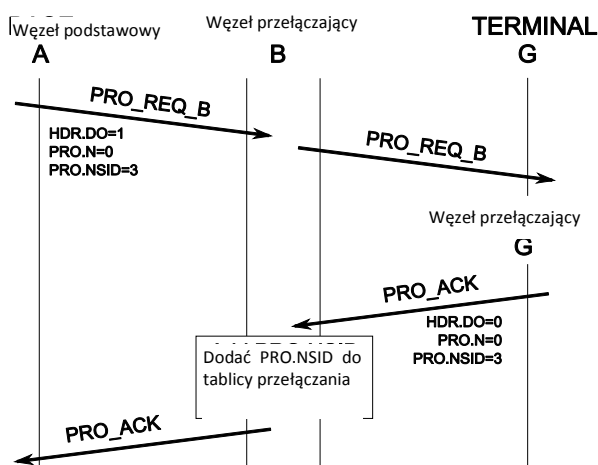
1243 Każdy węzeł przełączający posiada tablicę innych węzłów przełączających, które są podłączone za jego
1244 pośrednictwem do podsieci. Zachowywanie tych informacji jest wystarczające do przełączania, ponieważ
1245 ruch do/z węzłów terminala będzie również zawierał tożsamość odpowiednich węzłów przełączających
1246 (PKT.SID). Tym samym funkcja przełączania jest uproszczona pod tym względem, że wyczerpująca lista
1247 wszystkich podłączonych do niego węzłów terminala nie jest niezbędna.

1248 Węzły przełączające uruchamiają się przy braku wpisów w ich tablicach przełączania. Tablica przełączania
1249 jest dynamicznie aktualizowana w celu śledzenia pakietów kontrolnych promocji i degradacji
1250 przepływających w sieci. Nowa pozycja tworzona jest dla każdego zatwierdzenia promocji (PRO_ACK), które
1251 ma PKT.SID pasujący do SID węzła przełączającego lub dowolnych pozycji w tablicy przełączania. Podobnie
1252 pozycja odpowiadająca polu PRO.NSID usuwana jest po zatwierdzeniu żądania degradacji (PRO_DEM_x).



Rys. 27 - Przykład tablicy przełączania

Rys. 27 pokazuje przykład podsięci z zaznaczonymi pozycjami w tablicy przełączania poszczególnych węzłów przełączających. W tym przykładzie, gdy Węzeł serwisowy G odbiera pakiet PRO_REQ_B dla promocji, przekształca się on w węzeł przełączający. Jego identyfikatorem przełączenia będzie (PRO.NSID, 0) = (3, 0). Odbiór i przyjęcie PRO_REQ_B potwierdzane jest za pomocą PRO_ACK by G. Pośredni węzeł przełączający B wykryje HDR.DO=0, PKT.CTYPE=3, PKT.SID=1 oraz PRO.N=0, aby postanowić, że jest to PRO_ACK z jednego z węzłów serwisowych w jego własnej hierarchii przełączania. Węzeł B przekaze ten pakiet do węzła podstawowego i doda PRO.NSID do tablicy przełączania, jak pokazano na Rys. 28.



Rys. 28 - Uzupełniona tablica przełączania

Usuwanie pozycji tablicy przełączania jest bardziej złożone z powodu wznawiania prób. Po otrzymaniu zatwierdzenia degradacji (PRO_DEM_x), pozycja tabeli przełączającej odpowiadająca LSID oznaczana jest jako „do usunięcia”, a zegar uruchamiany jest z wartością $((macMaxCtReTx + 1) * macCtReTxTimer)$ sekund. Ten zegar zapewnia, że wszystkie retransmisje pakietów, które mogą korzystać z LSID, opuściły podsięć. Po upływie zaprogramowanego czasu pozycja tablicy przełączania zostanie usunięta.

1269 4.3.5.3 Proces przełączania

1270 Węzły przełączające przekazują ruch do ich domeny kontrolnej w sposób selektywny. Aby móc być
1271 przełączone, odebrane dane spełniają warunki wymienione poniżej. Jeśli warunki nie są spełnione, dane są
1272 cicho odrzucane.

1273 Aby zostać przełączone, pakiety połączenia pobierającego (HDR.DO=1) powinny spełniać dowolne z
1274 następujących warunków:

- 1275 • Węzeł docelowy pakietu jest podłączony do podsieci przez ten węzeł przełączający tj. PKT.SID jest
1276 równy SID tego węzła przełączającego lub jego tablica przełączania zawiera pozycję dla PKT.SID.
- 1277 • Pakiet ma punkt docelowy transmisji broadcast (PKT.LNID = 0x3FFF) i został wysłany przez
1278 przełączenie, przez które ten węzeł jest rejestrowany (PKT.SID=SID tego węzła przełączającego).
- 1279 • Pakiet ma punkt docelowy multicast (PKT.LNID=0x3FFE), został wysłany przez przełączenie, w
1280 którym zarejestrowany jest ten węzeł (PKT.SID=SID tego węzła przełączającego) i co najmniej jeden z
1281 węzłów serwisowych połączonych do podsieci przez ten węzeł przełączający jest członkiem
1282 wspomnianej grupy multicast, tj. LCID określa grupę, która jest wymagana przez dowolny węzeł niżej
1283 w tej hierarchii.

1284 Aby zostać przełączone, pakiety łącza ładowania (HDR.DO=0) powinny spełniać dowolne z następujących
1285 warunków:

- 1286 • Węzeł źródłowy pakietu jest podłączony do podsieci przez ten węzeł przełączający tj. PKT.SID jest
1287 równy SID tego węzła przełączającego lub jego tablica przełączania zawiera pozycję dla PKT.SID.
- 1288 • Pakiet ma punkt docelowy transmisji broadcast lub multicast (PKT.LNID = 0x3FFF lub 0x3FFE) i został
1289 wysłany przez węzeł zarejestrowany przez ten węzeł przełączający (PKT.SID=SID tego węzła
1290 przełączającego).

1291 Jeśli pakiet spełnia poprzednie warunki, powinien być przełączony. Dla pakietów unicast jedynym
1292 działaniem wykonywanym w czasie przełączania jest kolejgowanie w celu ponownego wysłania w jednostce
1293 PDU MAC z tym samym HDR.DO.

1294 W przypadku pakietów multicast lub broadcast PKT.SID należy zamienić na:

- 1295 • Identyfikator przełączenia lokalnego węzła przełączającego dla pakietów połączenia pobierającego.
- 1296 • SID węzła przełączającego dla pakietów łącza ładowania.

1297 4.3.5.4 Przełączanie pakietów Broadcast

1298 Przełączanie ramek MAC broadcast działa w inny sposób, niż przełączanie ramek MAC unicast. Ramki MAC
1299 broadcast identyfikowane są przez PKT.LNID=0x3FFF.

1300 Gdy HDR.DO=0, tj. pakiet jest pakietem łącza ładowania, jest on przesyłany jako unicast do węzła
1301 podstawowego. Przełączenie, które odbiera taki pakiet powinno zastosować zasady zasięgu, aby zapewnić,
1302 że pochodzi on z niższego poziomu i w ten sposób przełącza go w kierunku węzła podstawowego. Należy
1303 stosować zasady podane w punkcie 4.3.5.3.

1304 Gdy HDR.DO=01 tj. pakiet jest pakietem połączenia pobierającego, jest on przesyłany jako broadcast na
1305 kolejny poziom. Przełączenie, które odbiera taki pakiet powinno zastosować zasady zasięgu, aby zapewnić,

1306 że pochodzi on z wyższego poziomu i w ten sposób przelączy go dalej do swojej podsieci. Najbardziej
1307 odpornym schematem modulacji PHY i kodowania FEC przy maksymalnym poziomie mocy wyjściowej
1308 wdrożonym w urządzeniu powinny być stosowane tak, aby wszystkie urządzenia bezpośrednio podłączone
1309 do węzła przelączającego mogły odbierać pakiet. Należy stosować zasady podane w punkcie 4.3.5.3. Węzeł
1310 serwisowy powinien również przekazać pakiet do SAP MAC do aplikacji, które zarejestrowały się do
1311 odbierania pakietów broadcast za pomocą usługi MAC_JOIN.

1312 Gdy węzeł podstawowy odbiera pakiet broadcast z HDR.DO=0, powinien on przekazać pakiet do aplikacji,
1313 które zostały zarejestrowane, aby odbierać pakiety broadcast. Węzeł podstawowy powinien przesyłać
1314 pakiet jako pakiet połączenia pobierającego, tj. HDR.DO=1 za pomocą najbardziej stabilnego schematu
1315 modulacji PHY oraz kodowania FEC przy maksymalnym poziomie mocy wyjściowej i następujących zasadach
1316 podanych w punkcie 4.3.5.3.

1317 **4.3.5.5 Przelączanie pakietów Multicast**

1318 **4.3.5.5.1 Ogólne**

1319 Przelączanie pakietów multicast działa w bardzo podobny sposób do przelączania pakietów broadcast.
1320 Multicast jest rozszerzeniem broadcast. Jeśli węzeł przelączający nie wdraża multicastingu, powinien on
1321 traktować wszystkie pakiety multicast, tak jak pakiety broadcast.

1322 W tym punkcie opisano różne nazwy nagłówka MAC i pakietów. Odpowiednie definicje znajdują się w
1323 punkcie 4.4.2.

1324 **4.3.5.5.2 Tablica przelączania multicast**

1325 Węzły przelączające, które wdrażają multicasting powinny mieć tablicę przelączania multicast. Tabela ta
1326 zawiera wykaz identyfikatorów LCID grupy multicast, której członkowie podłączeni są do podsieci za
1327 pomocą węzła przelączającego. LCID ruchu multicast w kierunku połączenia pobierającego i łącza ładowania
1328 sprawdzane jest pod kątem zgodności z tablicą przelączania multicast. Ruch multicast przelączany jest
1329 jedynie, jeśli pozycja odpowiadająca LCID dostępna jest w tablicy. W przeciwnym razie ruch jest po cichu
1330 odrzucany.

1331 Tablica przelączania multicast jest ustanawiana i zarządzana przez kontrolę komunikatów dołączania i
1332 opuszczania multicast (pakiet kontrolny MUL), które przechodzą przez przelączanie. Należy zauważyć, że
1333 wiele węzłów serwisowych z hierarchii kontrolnej węzła przelączającego może być członkami tej samej
1334 grupy.

1335 Po udanym dołączeniu do grupy z węzła serwisowego w jej hierarchii kontrolnej, jeśli konieczne węzeł
1336 przelączający dodaje nową pozycję multicast do LCID grupy.

1337 Po wskazaniu udanego opuszczenia grupy przelączanie usuwa NID z pozycji przelączania multicast. Jeśli
1338 pozycja przelączania multicast nie ma związanego z nią NID, pozycja przelączania multicast jest natychmiast
1339 usuwana.

1340 Węzły przelączające powinny również sprawdzić pakiety utrzymania aktywności Keep-Alive przesyłane w
1341 górę. Gdy węzeł serwisowy, który również jest członkiem grupy multicast nie przeprowadzi pomyślnie
1342 procesu Keep-Alive, jego NID jest usuwany z wszystkich pozycji przelączania multicast i, jeśli konieczne,
1343 pozycja przelączania multicast jest usuwana.

Węzły przełączające powinny również stosować zegar do wyzwalania rzeczywistego usuwania pozycji przełączania. Zegar uruchamiany jest, gdy zapadnie decyzja, że pozycję należy usunąć. Zegar ten ma wartość $((macMaxCtReTx + 1) * macCtReTxTimer)$. Pozycja przełączania multicast jest usuwana jedynie gdy zadany czas upłynął. Umożliwia to węzłowi terminala na resetowanie wszelkich pozostałych pakietów multicast przed usunięciem połączenia, a wdrożenie węzła przełączającego jest uproszczone, ponieważ musi tylko przetworzyć MUL_LEAVE_B lub MUL_LEAVE_S (patrz podpunkt 4.4.5.10).

1350 **4.3.5.5.3 Proces przełączania pakietów multicast**

1351 Proces przełączania pakietu multicast zależy od kierunku pakietu.

1352 Gdy HDR.DO=0 i PKT.LNID=0x3FFE, tj. pakiet jest pakietem multicast łącza ładowania, jest on przesyłany
1353 jako unicast do węzła podstawowego. Węzeł przełączający, który odbiera taki pakiet powinien zastosować
1354 zasady zasięgu, aby zapewnić, że pochodzi on z niższego poziomu i w ten sposób przełącza go w kierunku
1355 węzła podstawowego. Nie wykonano filtrowania opartego na LCID. Wszystkie pakiety multicast są
1356 przełączane bez względu na pozycje przełączania multicast dla LCID. Stosować można prędkość kodowania
1357 najbardziej nadającą się do unicast oraz należy stosować zasady podane w punkcie 4.3.5.3.

1358 Gdy HDR.DO=1 i PKT.LNID=0x3FFE, tj. pakiet jest pakietem multicast połączenia pobierającego, stosowana
1359 jest tablica przełączania multicast. Jeśli istnieje jednostka z LCID odpowiadającym PKT.LCID w pakiecie,
1360 pakiet przełączany jest do części podsieci kontrolowanej przez to przełączenie. Najbardziej odpornym
1361 schematem modulacji PHY i kodowania FEC przy maksymalnym poziomie mocy powinny być stosowane tak,
1362 aby wszystkie urządzenia na niższym poziomie mogły odbierać pakiet. Należy stosować zasady podane w
1363 punkcie 4.3.5.3. Gdy węzeł serwisowy jest również członkiem grupy multicast, powinien on przekazać
1364 pakiet do aplikacji, które zostały zarejestrowane, aby odbierać pakiety multicast dla tej grupy.

1365 Gdy węzeł podstawowy odbiera pakiet multicast z HDR.DO=0 i jest członkiem grupy multicast, powinien on
1366 przekazać pakiet do aplikacji, które zostały zarejestrowane, aby odbierać pakiety multicast dla tej grupy.
1367 Węzeł podstawowy powinien przełączać pakiet multicast jeśli w jego tablicy przełączania znajduje się
1368 odpowiednia pozycja dla LCID transmitująca pakiet jako pakiet połączenia pobierającego, tj. HDR.DO=1 za
1369 pomocą najbardziej stabilnego schematu modulacji PHY oraz kodowania FEC przy maksymalnym poziomie
1370 mocy wyjściowej. Należy stosować zasady podane w punkcie 4.3.5.3.

1371 **4.3.6 Połączenia bezpośrednie**

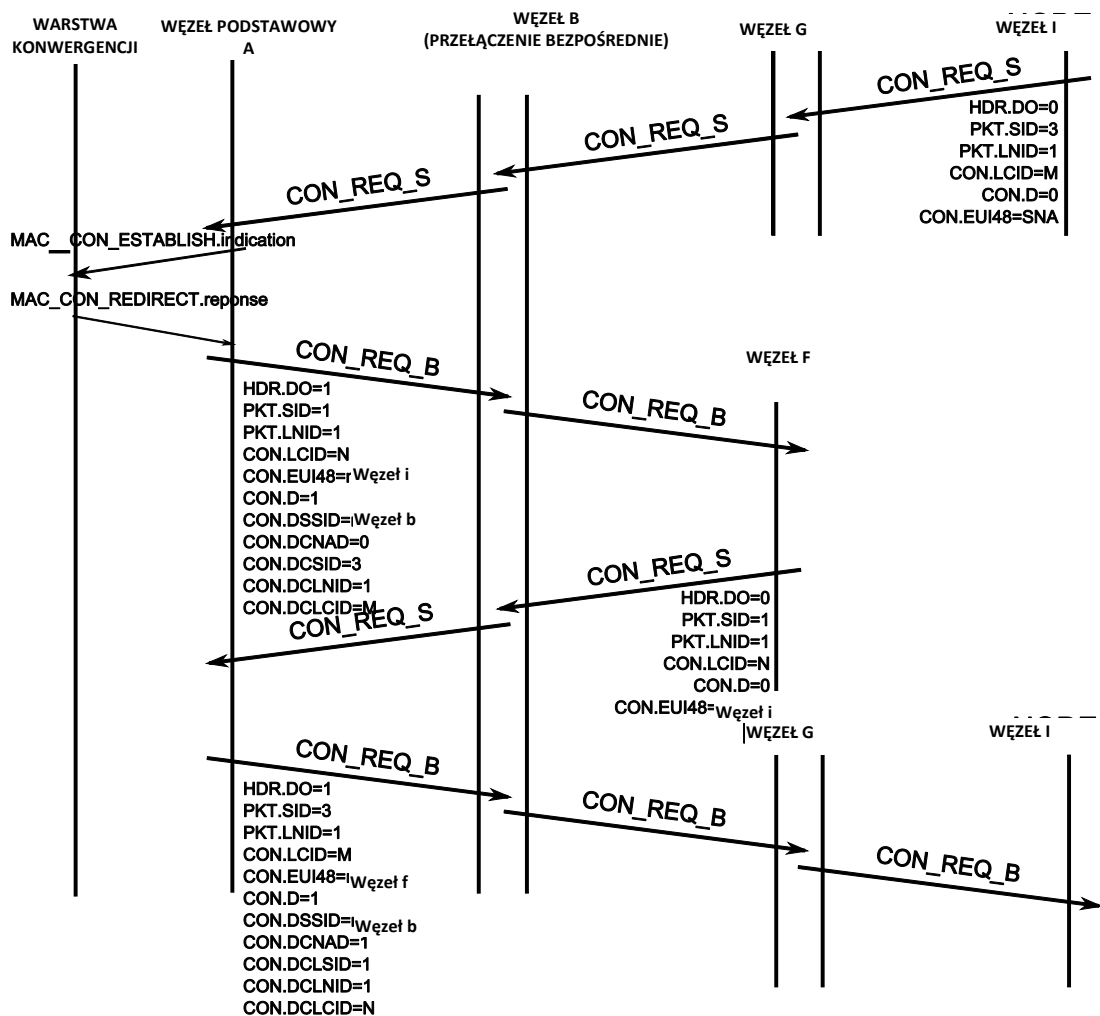
1372 **4.3.6.1 Ustanawianie połączenia bezpośredniego**

1373 Ustanawianie połączenie bezpośredniego trochę się różni od normalnego połączenia, mimo że używane są
1374 te same pakiety i procesy. Proces różni się, ponieważ wstępne żądanie połączenia może nie zostać
1375 zatwierdzone, chyba że jest już zatwierdzone przez węzeł docelowy. Różni się on również, ponieważ pakiety
1376 CON_REQ_B przenoszą informacje dla „przełączenia bezpośredniego”, aby zaktualizować „tablicę
1377 przełączania bezpośredniego”.

1378 Przełączanie bezpośrednie nie różni się od przełączania ogólnego. Jest to tylko logiczne rozróżnienie w
1379 identyfikacji pierwszego wspólnego przełączenia pomiędzy dwoma węzłami serwisowymi, które muszą
1380 komunikować się ze sobą. Należy zauważyć, że w związku z brakiem takiego wspólnego przełączania, węzeł
1381 podstawowy będzie działał jak przełączenie bezpośrednie.

Istnieją dwa różne scenariusze dla korzystających z połączeń bezpośrednich. Scenariusze te wykorzystują sieć pokazaną na Rys. 29.

Pierwszy scenariusz występuje, kiedy węzeł źródłowy nie zna adresu EUI-48 docelowego węzła serwisowego. Węzeł serwisowy inicjuje połączenie do węzła podstawowego, a warstwa konwergencji węzła podstawowego przekierowuje połączenie do odpowiedniego węzła serwisowego.



Rys. 29 – Połączenie przekierowane do nieznanego węzła serwisowego

Kroki ustanawiania połączenia bezpośredniego, zgodnie z Rys. 29 powinny wyglądać następująco:

- Gdy węzeł I próbuje nawiązać połączenie z węzłem F, powinien on wysłać normalne żądanie połączenia (CON_REQ_S).
- Następnie, ze względu na fakt, że węzeł podstawowy wie, że F jest docelowym węzłem serwisowym, powinien on wysłać żądania połączenia do F (CON_REQ_B). Pakiet ten będzie przenosić informacje do bezpośredniego przełączenia B, aby ująć to połączenie w swojej tablicy przełączania bezpośredniego.
- F może zaakceptować połączenie. (CON_REQ_S).
- Teraz, gdy połączenie z F jest w pełni ustanowione, węzeł podstawowy zaakceptuje połączenie z I (CON_REQ_B). Pakiet ten będzie przenosić informacje do bezpośredniego przełączenia B, aby ująć to połączenie w swojej tablicy przełączania bezpośredniego.

1400 Po zakończeniu tego procesu ustanawiania połączenia przełączenie bezpośrednie (węzeł B) powinno
 1401 zawierać tablicę przełączania bezpośredniego z pozycjami pokazanymi w Tabeli 8.

1402 **Tabela 8 - Przykład połączenia bezpośredniego: Tablica przełączania bezpośredniego węzła B**

Łącze ładowania			Połączenie pobierające			
SID	LNID	LCID	DSID	DLNID	DLCID	NAD
1	1	N	3	1	O	0
3	1	O	1	1	N	1

1403

1404 Tablica przełączania bezpośredniego powinna być aktualizowana za każdym razem, gdy przełączenie
 1405 otrzymuje pakiet kontrolny spełniający następujące wymagania:

- 1406 • Jest to pakiet CON_REQ_B: HDR.DO=1, CON.TYPE=1 i CON.N=0;
- 1407 • Zawiera on informacje „bezpośrednie”: CON.D=1;
- 1408 • Informacje bezpośrednie: CON.DSSID to identyfikator przełączenia SID samego przełączenia.

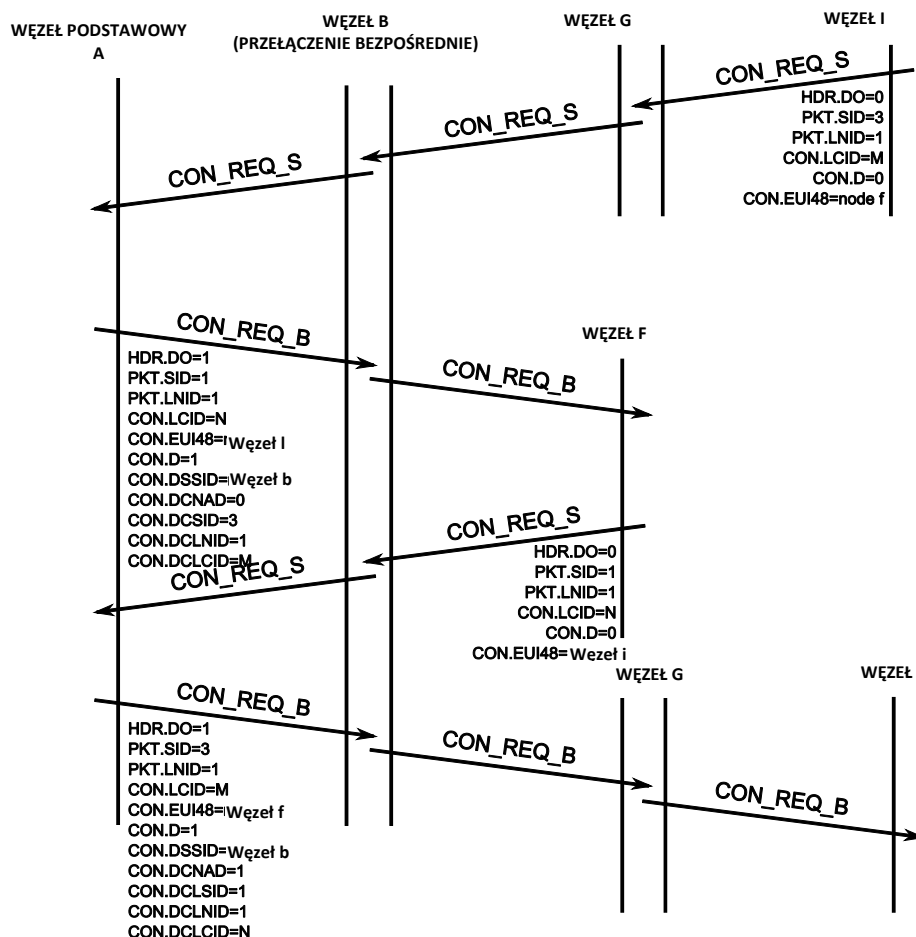
1409 Następnie tablica przełączania bezpośredniego jest aktualizowana tymi informacjami:

- 1410 • Łącze ładowania (SID, LNID, LCID) = (PKT.SID, PKT.LNID, CON.LCID);
- 1411 • Połączenie pobierające (SID, LNID, LCID, NAD) = (CON.DCSID, CON.DCLNID, CON.DCLCID,
 1412 CON.DCNAD).

1413 Aby usunąć pozycje, należy stosować pakiety zamykania połączenia.

1414 Drugi scenariusz do korzystania z połączeń bezpośrednich występuje, kiedy inicjujący węzeł serwisowy zna
 1415 już adres EUI-48 docelowego węzła serwisowego. W tym przypadku, zamiast używać adresu węzła
 1416 podstawowego, używa on adresu węzła serwisowego. W tym przypadku warstwa konwergencji węzła
 1417 podstawowego nie bierze udziału w procesie. Warstwa MAC węzła podstawowego łączy węzeł serwisowy I
 1418 bezpośrednio do węzła serwisowego F. Wynikające z tego połączenia pozycje tablicy przełączania są
 1419 identyczne jak w poprzednim przykładzie. Wymianę tych sygnałów pokazano na Rys. 30.

1420



1421

1422

Rys. 30 - Przykład połączenia bezpośredniego: ustanawianie połączenia ze znanym węzłem serwisowym

1423

4.3.6.2 Zwolnienie połączenia bezpośredniego

1424

1425

1426

1427

1428

Zwolnienie połączenia bezpośredniego pokazano na Rys. 31. Sygnaizowanie jest bardzo podobne do ustanawiania połączenia dla połączenia bezpośredniego. Pola D używane są do informowania przełączenia bezpośredniego, które pozycje należy usunąć. Tablica przełączania bezpośredniego powinna być aktualizowana za każdym razem, gdy przełączenie otrzymuje pakiet kontrolny spełniający następujące wymagania:

1429

1430

1431

- Jest to pakiet CON_CLOSE_B: HDR.DO=1, CON.TYPE=1 i CON.N=1;
- Zawiera on informacje „bezpośrednie”: CON.D=1;
- Informacje bezpośrednie: CON.DSSID to identyfikator przełączenia SID samego przełączenia.

1432

Następnie usuwana jest pozycja tablicy przełączania bezpośredniego zawierająca następujące informacje:

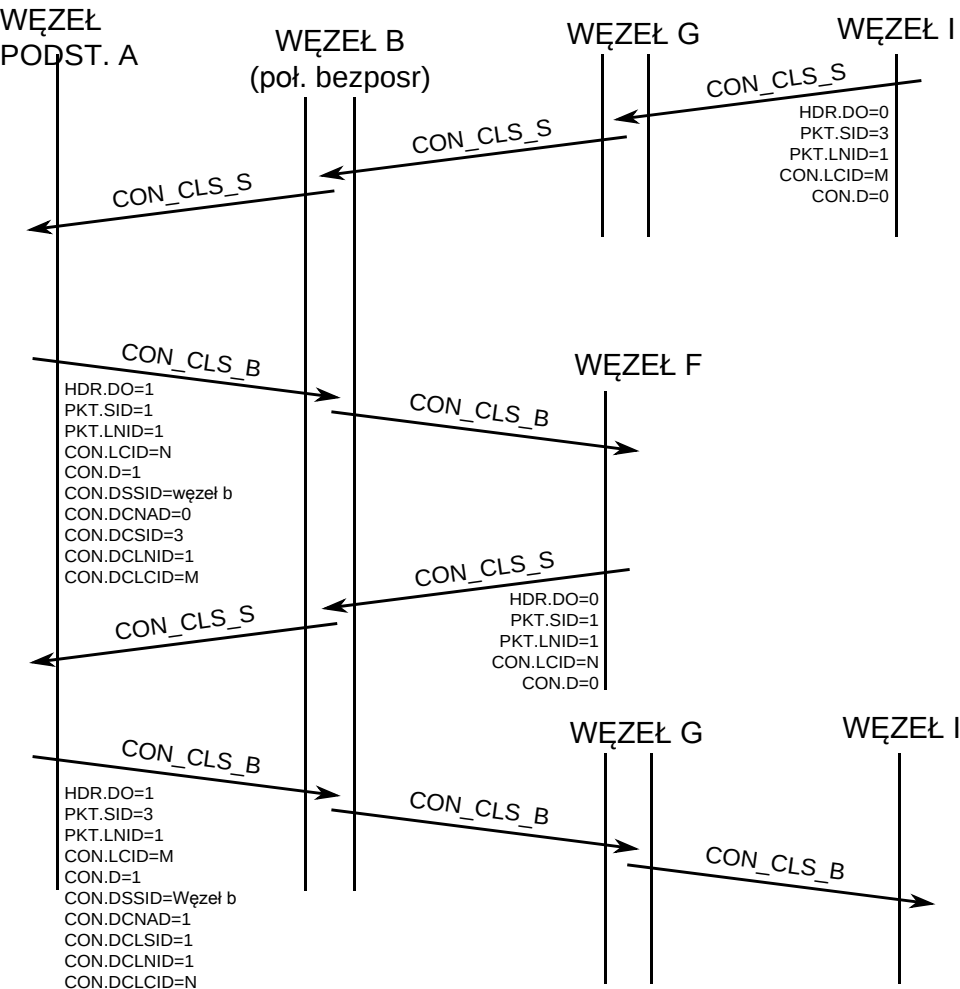
1433

1434

1435

- Łącze ładowania (SID, LNID, LCID) = (PKT.SID, PKT.LNID, CON.LCID);
- Połączenie pobierające (SID, LNID, LCID, NAD) = (CON.DCSID, CON.DCLNID, CON.DCLCID, CON.DCNAD).

1436



Rys. 31 - Zwolnienie połączenia bezpośredniego

4.3.6.3 Przełączenie połączenia bezpośredniego

Jak wyjaśniono w punkcie 4.3.5.3, normalny mechanizm przełączania jest przeznaczony do przekazywania danych komunikacyjnych między węzłem podstawowym, a każdym węzłem serwisowym. „Przełączanie bezpośrednie” jest mechanizmem umożliwiającym dwóm węzłom komunikowanie się między sobą, przełączanie pakietów w sposób lokalny, tj. bez przechodzenia przez węzeł podstawowy. Nie jest to inna forma przełączania pakietów, lecz raczej dodatkowa funkcja ogólnego procesu przełączania.

Pierwsze udostępnione przełączenie w ścieżki, które prowadzą z dwóch węzłów serwisowych do węzła podstawowego będzie nazwane „przełączeniem bezpośrednim” dla połączeń pomiędzy wspomnianymi węzłami. Jest to przełączenie, które będzie miało możliwość wykonania bezpośredniego przełączania, aby zapewnić skuteczną komunikację pomiędzy dwoma węzłami. W przypadku szczególnym każde przełączenie jest „bezpśrednim przełączeniem” pomiędzy sobą a każdym węzłem, który znajduje się niżej w hierarchii.

Tablica przełączania bezpośredniego jest tablicą, którą powinno zawierać każde przełączenie w celu przeprowadzania przełączania bezpośredniego. Każda pozycja w tej tablicy jest połączeniem bezpośrednim, które musi być bezpośrednio przełączane. Reprezentowana jest ona przez źródłowy identyfikator CID oraz docelowy identyfikator CID połączenia bezpośredniego. Nie jest to zapis identyfikatora połączenia

znajdującego się niżej w hierarchii, ale zawiera jedynie te połączenia, które powinny być przełączane bezpośrednio. Umiejętność węzła docelowego do otrzymywania połączonych pakietów powinna również umieszczona zostać w „tablicy przełączania bezpośredniego” w celu wypełnienia pola PKT.NAD.

4.3.6.4 Operacja przełączania bezpośredniego

Jeśli przełączenie odbierze ramkę MAC łączy ładowania (HDR.DO=0), które ma zostać przełączone (informacje na temat wymogów - patrz punkt 4.3.5.3) oraz jej adres w tablicy przełączania bezpośredniego, procedura wygląda następująco:

- Zmiana (SID, LNID, LCID, NAD) przez element połączenia pobierającego pozycji w tablicy przełączania bezpośredniego.
- Kolejowanie pakietu do wysłania jako pakiet połączenia pobierającego (HDR.DO=1).

4.3.7 Agregacja pakietów

4.3.7.1 Ogólne

GPDU może zawierać jeden lub więcej pakietów. Funkcjonalność ujmowania kilku pakietów w GPDU nazywa się agregacją pakietów. Agregacja pakietów stanowi opcjonalną część specyfikacji, a urządzenia nie muszą wdrażać jej w celu zachowania zgodności ze specyfikacją. Sugeruje się jednak, aby urządzenia wdrażały agregację pakietów w celu usprawnienia skuteczności warstwy MAC.

Aby zachować kompatybilność pomiędzy urządzeniami, które wdrażają agregację pakietów i tymi, które tego nie robią, niezbędna jest gwarancja, że agregacja nie będzie miała miejsca dla pakietów, których ścieżka transportu danych z/do węzła podstawowego przecina pośrednie węzły (pośredni węzeł), które nie wdrażają (który nie wdraża) tej funkcji. Informacje o możliwości agregacji ścieżki transportu danych są wymieniane podczas procesu rejestracji (4.6.1). Węzeł serwisowy rejestracji powiadamia węzeł podstawowy o tej możliwości w polu REG.CAP_PA (1-bitowe, patrz Tabela 14) swojego komunikatu REG_REQ. Dostaje on informacje zwrotne od węzła podstawowego o możliwości agregacji całej ścieżki transportu połączenia pobierającego w polu REG.CAP_PA komunikatu REG_RSP.

Na podstawie wstępnych informacji wymienianych w czasie rejestracji, każdy kolejny pakiet danych w obu kierunkach zawiera informacje na temat agregacji w polu PKT.NAD. W kierunku połączenia pobierającego węzeł podstawowy będzie odpowiadać za wypełnienie pola PKT.NAD na podstawie wartości przekazanej do docelowego węzła serwisowego w polu REG.CAP_PA komunikatu REG_RSP. Podobnie, w przypadku danych łączy ładowania źródłowy węzeł serwisowy wypełni pole PKT.NAD na podstawie pola REG.CAP_PA odebranego w początkowym REG_RSP z węzła podstawowego. Ostatnie przełączenie powinno skorzystać z pola PKT.NAD w celu uniknięcia agregacji pakietów podczas przekazywania dalej pakietu do docelowych węzłów serwisowych bez możliwości agregacji pakietu. Pośrednie węzły przełączające powinny zawierać informacje na temat możliwości agregacji w tablicach przełączania i nie powinny łączyć pakietów, gdy wiadome jest, że węzeł przełączający kolejnego poziomu nie obsługuje tej funkcji.

Urządzenie, które wdrażają agregację pakietu powinny zapewnić, że rozmiar MSDU składający się z agregatów nie przekracza maksymalnej przepustowości najbardziej odpornego schematu transmisji seryjnej PHY. Najbardziej odporny schemat transmisji odnosi się do najbardziej odpornego połączenia schematu modulacji i kodowania splotowego.

1493 **4.3.7.2 Agregacja pakietu podczas przełączania**

1494 Węzły przełączające przechowują informację o możliwości agregacji pakietów przez wszystkie pozycje w ich
1495 tablicy przełączania, tj. wszystkich przełączeniach podłączonych przez te węzły do podsieci. Informacja ta jest
1496 następnie wykorzystywana podczas przełączania ruchu do/z podłączonych węzłów przełączających.

1497 Uprawnienie do agregacji pakietów przez łączący węzeł przełączeniowy jest zarejestrowane w każdym
1498 węźle przełączającym w momencie jego promocji poprzez wykrywanie stosownych informacji w
1499 komunikacie PRO_ACK.

- 1500 • Jeśli PKT.SID w komunikacie PRO_ACK jest taki sam jak w węźle przełączającym, promowany węzeł
1501 jest podłączany bezpośrednio do wspomnianego węzła przełączającego. Uprawnienie do agregacji
1502 tego nowego węzła przełączającego jest zarejestrowane jako takie same, jak w PKT.NAD pakietu
1503 PRO_ACK.
- 1504 • Jeśli PKT.SID w komunikacie PRO_ACK różni się od identyfikatora węzła przełączającego, oznacza to,
1505 że promowany węzeł jest podłączany pośrednio do tego przełączenia. Uprawnienie do agregacji
1506 pakietów tego nowego węzła przełączającego będzie takie same jak uprawnienie zarejestrowane dla
1507 tego przełączenia bezpośredniego, tj. PKT.SID.

1508 Agregacja podczas przełączania pakietów w kierunku łącza ładowania wykonywana jest gdy węzeł
1509 wykonujący przełączenie wie, że jego ścieżka łącza ładowania jest w stanie obsłużyć połączone pakiety na
1510 podstawie informacji wymienianych podczas rejestracji (pole REG.CAP_PA w komunikacie REG_RSP).

1511 Pakiety połączenia pobierającego są łączone poprzez analizę następujących informacji:

- 1512 • Jeśli identyfikator PKT.SID jest taki sam, jak dla węzła przełączającego, jest to ostatni poziom
1513 przełączania, a pakiet dotrze do swojego miejsca docelowego. W tym przypadku pakiet może być
1514 połączony, jeśli PKT.NAD=0.
- 1515 • Jeśli PKT.SID różni się, nie jest to ostatni poziom, a pakiet otrzyma kolejne przełączenie. Informacje o
1516 tym, czy pakiet może zostać zagregowany powinny być pozyskiwane z tablicy przełączania.

1517 **4.3.8 Zabezpieczenie**

1518 **4.3.8.1 Ogólne**

1519 Funkcja zabezpieczeń zapewnia warstwie MAC prywatność, uwierzytelnienie i integralność danych za
1520 pomocą metody bezpiecznego połączenia i polityki zarządzania kluczami. Wszystkie pakiety muszą
1521 korzystać z wynegocjowanego profilu zabezpieczeń. Jedynymi wyjątkami od tej reguły są wiadomości
1522 kontrolne REG i SEC oraz BPDU i PNPDU, które są przesyłane bez szyfrowania.

1523 **4.3.8.2 Profile zabezpieczeń**

1524 Kilka profili zabezpieczeń służy do zarządzania różnymi potrzebami w zakresie zabezpieczeń, które mogą
1525 wystąpić w różnych środowiskach sieciowych. Ta wersja specyfikacji opisuje dwa profile zabezpieczeń i
1526 pozostawia miejsce na dodanie maksymalnie dwóch nowych profili zabezpieczeń w przyszłych wersjach.

1527 4.3.8.2.1 Profil zabezpieczeń 0

1528 Komunikacja z Profilem zabezpieczeń 0 opiera się na transmisji jednostek SDU warstwy MAC bez
1529 szyfrowania. Ten profil może być używany w scenariuszach, gdzie górne warstwy komunikacyjne
1530 zapewniają dostateczne zabezpieczenia lub gdzie zabezpieczenia nie stanowią znaczącego wymagania.

1531 4.3.8.2.2 Profil zabezpieczeń 1**1532 4.3.8.2.2.1 Ogólne**

1533 Profil zabezpieczeń 1 opiera się na 128-bitowym szyfrowaniu AES danych i jego powiązanej kontroli. Ten
1534 profil jest określony w celu spełnienia wszystkich wymogów zabezpieczeń:

- 1535 • Prywatność gwarantowana jest poprzez samo szyfrowanie i przez fakt, że klucz szyfrowania
1536 utrzymywany jest w tajemnicy.
- 1537 • Uwierzytelnianie jest gwarantowane przez fakt, że każdy węzeł ma swój tajny klucz znany tylko przez
1538 sam węzeł i do węzła podstawowy.
- 1539 • Integralność danych jest gwarantowana przez fakt, że treść jest szyfrowana przez CRC.

1540 4.3.8.2.2.2 Prymitywy kryptograficzne

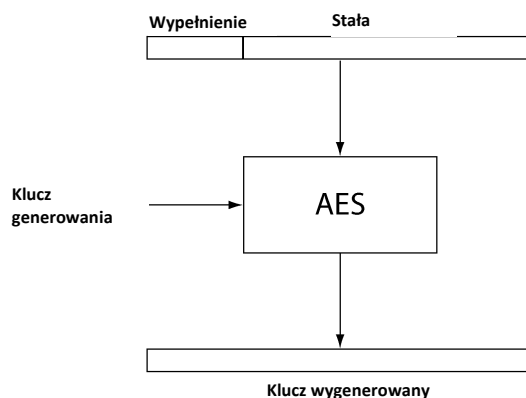
1541 Algorytm szyfrowania stosowany w tej specyfikacji to AES, jak określono w FIPS197. Specyfikacja opisuje
1542 algorytm z trzema możliwymi rozmiarami kluczy. 128-bitowy klucz tajny reprezentuje wysoki poziom
1543 bezpieczeństwa dla zachowania prywatności aż do 2030 i powyżej, w sposób określony w SP800-57, strona
1544 66, tabela 4.

1545 AES jest używany zgodnie z tzw. ECB, jak określono w SP800-38A. Jest to tryb szyfrowania blokowego, w
1546 którym zwykły tekst jest podzielony na bloki 128-bitowe. Wypełnienie stosowane jest, jeśli ostatni blok jest
1547 mniejszy niż 128 bitów. Wypełnienie jest realizowane z dodaniem bitu równego 1 oraz tylu zer, ile
1548 niezbędne jest do osiągnięcia długości ciągu szyfrowanego jako wielokrotność 128 bitów. Szyfrowanie
1549 przeprowadzane jest po jednym bloku na raz za pomocą tego samego klucza roboczego dla wszystkich
1550 danych.

1551 4.3.8.2.2.3 Algorytm wyprowadzania klucza

1552 Metodą wyprowadzania kluczy roboczych z kluczy tajnych jest zastosowanie algorytmu AES do stałej (C)
1553 jako tekstu niezakodowanego i klucza generowania (GK) jako klucza szyfrowania. Jeśli stała jest krótsza niż
1554 128 bitów, musi zostać wyrównana do LSB, jak pokazano na Rys. 32. Różne równania wyprowadzania klucza
1555 określone w kolejnych podpunktach są zgodne z konwencją:

1556 *Wygenerowany klucz = AES_enc (Klucz generowania, Stała)*



Rys. 32 - Koncept wyprowadzania klucza

4.3.8.3 Negocjowanie profilu zabezpieczeń

Wszystkie dane MAC, w tym jednostki sygnalizujące PDU (wszystkie pakiety kontrolne MAC określone w punkcie 4.4.5) korzystają z tego samego profilu zabezpieczeń. Ten profil negocjowany jest w czasie rejestracji urządzenia. W komunikacie REG_REQ Terminal wskazuje profil zabezpieczeń, który jest w on w stanie obsłużyć w polu REG.SPC. Węzeł podstawowy może zatwierdzić ten profil zabezpieczeń oraz proces rejestracji poprzez odesłanie REG_RSP o tej samej wartości REG.SPC. Węzeł podstawowy może również zatwierdzić samą rejestrację, jednakże ustawia on REG.SPC na 0, co wskazuje, że konieczne jest zastosowanie profilu zabezpieczeń 0. Alternatywnie węzeł podstawowy może odrzucić rejestrację jeśli terminal nie zapewni dopuszczalnego profilu zabezpieczeń.

Zaleca się, aby terminal najpierw spróbował rejestracji za pomocą najwyższego profilu zabezpieczeń jaki obsługuje i korzystał z niższych profili jedynie, gdy węzeł podstawowy odrzucił żądanie rejestracji.

4.3.8.4 Hierarchia kluczy

4.3.8.4.1 Profil zabezpieczeń 0

Nie dotyczy.

4.3.8.4.2 Profil zabezpieczeń 1

Węzły serwisowe i węzły podstawowe korzystają z zestawu trzech kluczy roboczych do szyfrowania danych. Klucze i ich zastosowanie:

Początkowy klucz roboczy (WK0): Ten klucz ma ograniczony zasięg i jest używany do odszyfrowywania pól REG.SNK i REG.AUK komunikatu REG_RSP. WK0 jest więc używany przez węzeł serwisowy w stanie funkcjonalnym *Rozłączony*. Klucz obliczany jest za pomocą następującego wzoru:

$$WK0 = \text{AES_enc}(USK, 0)$$

Klucz roboczy (WK): Ten klucz jest wykorzystywany do szyfrowania wszystkich danych unicast, które są przesyłane z węzła podstawowego do węzła serwisowego i odwrotnie. Każdy zarejestrowany węzeł serwisowy ma unikalny klucz roboczy znany tylko węzłowi podstawowemu i sobie. Klucz WK obliczany jest w następujący sposób:

$$WK = \text{AES_enc}(USK, \text{Losowy ciąg odbierany w SEC.RAN})$$

1585 **Klucz roboczy podsieci (SWK):** Klucz roboczy podsieci współdzielony jest przez całą podsieć. Aby zapewnić
1586 bezpieczeństwo tego klucza, nigdy nie jest on transmitowany przez kanał fizyczny, ale jest obliczany z
1587 innych kluczy, które są przesyłane jako zaszyfrowane w REG i niezabezpieczone w pakietach kontrolnych
1588 SEC. Klucz SWK będzie używany do szyfrowania:

- 1589 • Dane broadcast, w tym pakiety kontrolne MAC broadcast.
- 1590 • Dane Multicast.
- 1591 • Dane unicast, które są przesyłane połączeniami bezpośrednimi, tj. bez udziału węzła podstawowego.

1592 Klucz SWK obliczany jest w następujący sposób:

1593 $SWK = AES_enc(SNK, \text{Losowy ciąg odbierany w SEC.SNK})$

1594 Klucze WK i SWK mają ograniczoną ważność czasową związaną z okresem generowania losowych sekwencji.
1595 Losowa sekwencja jest generowana i dystrybuowana przez węzeł podstawowy co najmniej co
1596 $MACRandSeqChgTime$ sekund przez pakiet kontrolny SEC. Jeśli urządzenie nie otrzyma aktualizacji losowej
1597 sekwencji w przeciągu $2 * MACRandSeqChgTime$, należy uznać, że klucze WK i SWK nie są już prawidłowymi
1598 kluczami. Brak dostępności WK spowoduje bardzo ograniczoną funkcjonalność wyrejestrowywania węzła
1599 serwisowego z podsieci. Zaleca się zatem, aby w takich przypadkach węzły serwisowe wyrejestrowywały się
1600 z podsieci i inicjowały procedurę wyrejestrowywania.

1601 Procedury wyprowadzenia klucza zostały opracowane tak, aby były procedurami pośrednimi i
1602 wielostopniowymi w celu zapewnienia bezpieczeństwa. Parametry biorące udział w wyprowadzaniu kluczy
1603 roboczych zdefiniowano poniżej.

1604 **Klucz główny (MK1, MK2).** W niniejszej specyfikacji zdefiniowane zostały dwa klucze główne (MK1 i MK2).
1605 Klucz MK1 służy do obliczania klucza DSK. Klucz MK2 służy do obliczania KDIV. Oba te klucze zarządzane są
1606 w węźle podstawowym przez działania zależące od wdrożenia, które wykraczają poza zakres niniejszej
1607 specyfikacji. Określanie dwóch kluczy głównych sprawia, że proces generowania klucza USK jest procesem
1608 dwuetapowym, tj. wyprowadzenie DSK i KDIV na pierwszym etapie oraz użycie ich do wyprowadzenia USK
1609 na drugim etapie. Należy zauważyć, że DSK i KDIV są unikalne dla każdego rejestrującego węzła
1610 serwisowego.

1611 **Klucz tajny urządzenia (DSK).** DSK jest unikalny dla każdego węzła serwisowego w podsieci i jest kodowany
1612 na sztywno w urządzeniu w czasie produkcji. Klucz tajny urządzenia DSK jest stały przez cały okres działania
1613 węzła serwisowego. Węzeł podstawowy korzysta z MK1 do wyprowadzenia kluczy DSK właściwych dla
1614 węzła serwisowego za pomocą następującego równania:

1615 $DSK = AES_enc(MK1, UI)$

1616 **Dywersyfikator kluczy (KDIV).** Liczba ta jest również unikalna dla każdego węzła serwisowego, ale w
1617 przeciwieństwie do DSK, nie musi ona być stałą dla całego okresu eksploatacji węzła serwisowego. Klucz
1618 KDIV jest umieszczany w każdym węźle serwisowym sposobami wykraczającymi poza zakres niniejszej
1619 specyfikacji. Węzeł podstawowy oblicza KDIV właściwy dla połączenia za pomocą równania:

1620 $KDIV = AES_enc(MK2, UI)$

1621 **Unikalny tajny klucz (USK).** USK stosowany jest do wyprowadzenia WK0 i WK zgodnie z powyższymi
1622 równaniami. Klucz USK jest z kolei obliczany poprzez zastosowanie AES do KDIV za pomocą DSK jako klucza
1623 generowania, jak pokazano na poniższym równaniu. Należy zauważyć, że jest to proces jednoetapowy w
1624 węźle serwisowym, ponieważ oba klucze KDIV i DSK są już znane lub dostarczone, ale proces trzyetapowy w
1625 węźle podstawowym. Pierwsze dwa etapy w węźle podstawowym polegają na wyprowadzeniu DSK i KDIV
1626 za pomocą odpowiednio MK1 i MK2;

1627 $USK = AES_enc(DSK, KDIV)$

1628 **Unikalny identyfikator (UI):** UI węzła serwisowego powinien być jego identyfikatorem EUI-48.

1629 **4.3.8.5 Dystrybucja i zarządzanie kluczami**

1630 Profil zabezpieczeń dla ruchu danych negocjowany jest, gdy urządzenie jest rejestrowane. Pakiet kontrolny
1631 REG zawiera określone pola wskazujące profil zabezpieczeń dla odpowiednich urządzeń. Wszystkie
1632 połączenia do/z urządzenia powinny być wymagane do stosowania profilu zabezpieczeń wynegocjowanego
1633 w czasie rejestracji. Profile zabezpieczeń w wielu połączeniach z udziałem tego samego urządzenia nie
1634 mogą się różnić. Jedynym wyjątkiem od tej reguły jest węzeł podstawowy.

1635 Klucz SWK jest stosowany jako klucz roboczy dla ruchu niebędącego ruchem unicast, a połączenia
1636 bezpośrednie nigdy nie są przesyłane przez kanał fizyczny w formie niezaszyfrowanej. Komunikaty
1637 zabezpieczeń broadcast przesyłane przez węzeł podstawowy (i przekazywane przez wszystkie węzły
1638 przełączające) w regularnych odstępach czasu zawierają losowe klucze dla ruchu unicast i pozostałego
1639 ruchu. Gdy urządzenie początkowo rejestruje się w podsięci, odpowiedź REG z węzła podstawowego
1640 zawiera losową sekwencję stosowaną do wyprowadzania klucza roboczego dla ruchu unicast. Po
1641 komunikacie REG następuje komunikat SEC unicast z węzła podstawowego do urządzenia rejestrującego.

1642 **4.3.8.6 Szyfrowanie**

1643 **4.3.8.6.1 Profil zabezpieczeń 0**

1644 Nie dotyczy.

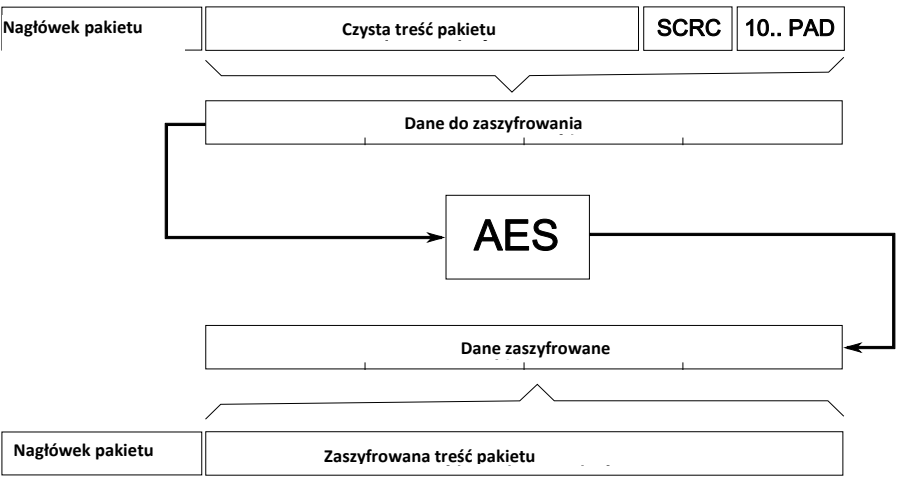
1645 **4.3.8.6.2 Profil zabezpieczeń 1**

1646 Połączenia pracujące z „Profiłem zabezpieczeń 1” zawsze przysyłać będą CRC z każdym pakietem. To pole
1647 nazywane jest SCRC (kontrolą CRC zabezpieczeń) i obliczane jest za pomocą niezaszyfrowanej treści pakietu.
1648 SCRC pomaga potwierdzać integralność pakietu na podstawie odszyfrowania po stronie odbiorczej.

1649 Kontrolę CRC należy obliczyć jako pozostałość z dzielenia (Modulo 2) przez wielomian generujący
1650 $g(x) = x^8 + x^2 + x + 1$ wielomianu x^8 pomnożony przez zaszyfrowaną treść pakietu.

1651 Blok danych uzyskanych poprzez konkatencję niezaszyfrowanej treści pakietu, a obliczona kontrola SCRC
1652 jest wypełniana 1, po której następuje tyle zer ile to konieczne do uzyskania wielu 128, a następnie
1653 dzielonych na bloki 128-bitowe. 1 umieszczana jako pierwszy bit wypełnienia jest używana do wykrywania
1654 początku wypełnienia w nadajniku bez powiadamiania o liczbie wypełnionych bitów.

1655 Każdy blok 128-bitowy jest zaszyfrowany za pomocą algorytmu AES przy pomocy ważnego klucza
1656 roboczego. Wynikiem tego procesu szyfrowania jest zaszyfrowana treść pakietu.



Rys. 33 - Algorytm szyfrowania Profilu bezpieczeństwa 1

4.4 Format MAC PDU

4.4.1 Ogólne

Istnieją różne rodzaje PDU MAC do różnych celów.

4.4.2 Ogólna jednostka MAC PDU

4.4.2.1 Ogólne

Większość ruchu podsieci składa się z Ogólnych jednostek MAC PDU (GPDU). Jednostki GPDU są stosowane dla całego ruchu danych i większości ruchu kontrolnego. Wszystkie pakiety kontrolne MAC przesyłane są jako GPDU.

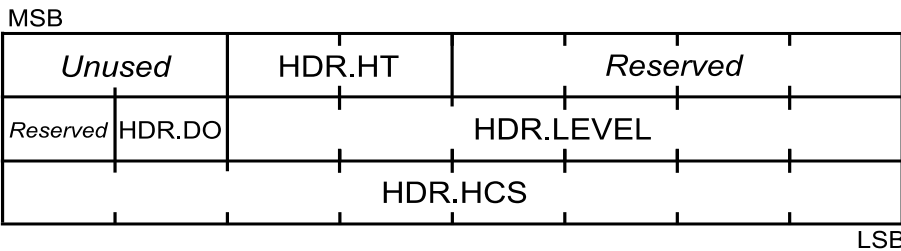
Skład GPDU pokazano na Rys. 34. Składa się ona z ogólnego nagłówka MAC, po którym następuje jeden lub więcej pakietów MAC i 32-bitowa kontrola CRC dołączana na końcu.



Rys. 34 - Ogólny format PDU MAC

4.4.2.2 Ogólny nagłówek MAC

Format ogólnego nagłówka MAC przedstawiono na Tabela 9. Rozmiar ogólnego nagłówka MAC wynosi 3 bajty. Tabela 9 zawiera każde pole ogólnego nagłówka MAC.



Rys. 35 - Ogólny nagłówek MAC

1676

Tabela 9 - Pola ogólnego nagłówka MAC

Nazwa	Długość	Opis
Unused (Nieużywany)	2 bity	Niewykorzystane bity, które zawsze wynoszą 0; ujęte do wyrównania z polem MAC_H w nagłówku PDU (Punkt 3.4.3).
HDR.HT	2 bity	Typ nagłówka. HDR.HT = 0 dla GPDU
Reserved (Zarezerwowany)	5 bitów	Zawsze 0 dla tej wersji specyfikacji. Zarezerwowany do użytku w przyszłości.
HDR.DO	1 bit	Downlink/Uplink (Połączenie pobierające/łącze ładowania). - HDR.DO=0 jeśli PDU MAC jest połączeniem pobierającym. - HDR.DO=0 jeśli PDU MAC jest łączem ładowania.
HDR.LEVEL	6 bitów	Poziom PDU w hierarchii przełączania. Pakiety między poziomem 0 i węzłem podstawowym mają HDR.LEVEL=0. Pakiety pomiędzy poziomami k i k-1 to HDR.LEVEL=k. - Jeśli HDR.DO=0, HDR.LEVEL oznacza poziom nadawcy tego pakietu. - Jeśli HDR.DO=1, HDR.LEVEL oznacza poziom odbiorcy tego pakietu.
HDR.HCS	8 bitów	Sekwencja Kontrolna Nagłówka. Pole do wykrywania błędów w nagłówku i sprawdzania, czy ta jednostka PDU MAC pochodzi z tej podsieci. Nadajnik powinien obliczyć kontrolę CRC adresu SNA połączonego z 2 pierwszymi bajtami nagłówka i wstawić wynik w pole HDR.HCS (ostatni bajt nagłówka). Kontrolę CRC należy obliczyć jako pozostałość z dzielenia (Modulo 2) wielomianu $M(x)=x^8+x$ przez wielomian generujący $g(x)=x^8+x^2+x+1$. $M(x)$ jest wielomianem wejściowym, który jest utworzony przez ciąg bitów konkatencji SNA, oraz nagłówek bez pola HDR.HCS, a najbardziej znaczący bit z ciągu bitów jest współczynnikiem najwyższego rzędu $M(x)$.

1677 **4.4.2.3 Struktura pakietu**

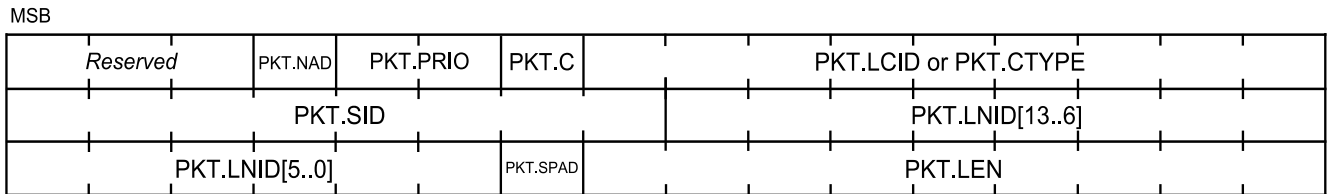
1678 Pakiet składa się z nagłówka pakietu i treści pakietu. Rys. 36 pokazuje strukturę.

1679
1680



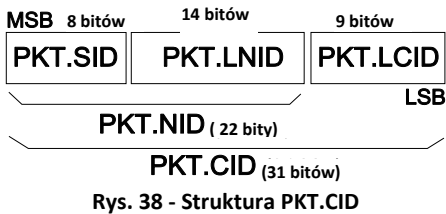
Rys. 36 - Struktura pakietu

1681 Nagłówek pakietu ma długość 6 bajtów, a jego skład pokazano na Rys. 37. Tabela 10 podaje opis każdego
1682 pola.



Rys. 37 – Nagłówek pakietu

Dla uproszczenia tekst zawiera odniesienia do pól PKT.NID jako skład PKT.SID i PKT.LNID. Pole PKT.CID określa się również jako połączenie PKT.NID oraz PKT.LCID. Skład tych pól został opisany na Rys. 38.



Rys. 38 - Struktura PKT.CID

Tabela 10 – Pola nagłówka pakietu

Nazwa	Długość	Opis
Reserved	3 bity	Zawsze 0 dla tej wersji specyfikacji. Zarezerwowany do użytku w przyszłości.
PKT.NAD	1 bit	Brak agregacji w miejscu docelowym - Jeśli PKT.NAD=0, pakiet może być połączony z innymi pakietami w punkcie docelowym. - Jeśli PKT.NAD=1, pakiet nie może być połączony z innymi pakietami w punkcie docelowym.
PKT.PRIO	2 bity	Wskazuje priorytet pakietu od 0 do 3.
PKT.C	1 bit	Kontrola - Jeśli PKT.C=0, jest to pakiet danych. - Jeśli PKT.C=1, to jest pakiet kontrolny.
PKT.LCID / PKT.CTYPE	9 bitów	Identyfikator połączenia lokalnego lub typ kontroli - Jeśli PKT.C=0, PKT.LCID oznacza Identyfikator połączenia lokalnego pakietu danych. - Jeśli PKT.C=1, PKT.CTYPE reprezentuje typ pakietu kontrolnego.
PKT.SID	8 bitów	Identyfikator przełączenia - Jeśli HDR.DO=0, PKT.SID oznacza identyfikator SID źródła pakietu. - Jeśli HDR.DO=1, PKT.SID oznacza identyfikator SID pakietu docelowego.

Nazwa	Długość	Opis
PKT.LNID	14 bitów	Identyfikator węzła lokalnego. - Jeśli HDR.DO=0, PKT.LNID oznacza LNID źródła pakietu - Jeśli HDR.DO=1, PKT.LNID oznacza LNID pakietu docelowego.
PKT.SPAD	1 bit	Wskazuje, czy wypełnienie zostaje wstawione podczas szyfrowania treści. Należy zauważyć, że ten bit jest poprawny jedynie, gdy stosowany jest Profil zabezpieczeń 1 (patrz 4.3.8.2.2).
PKT.LEN	9 bitów	Długość treści pakietu w bajtach.

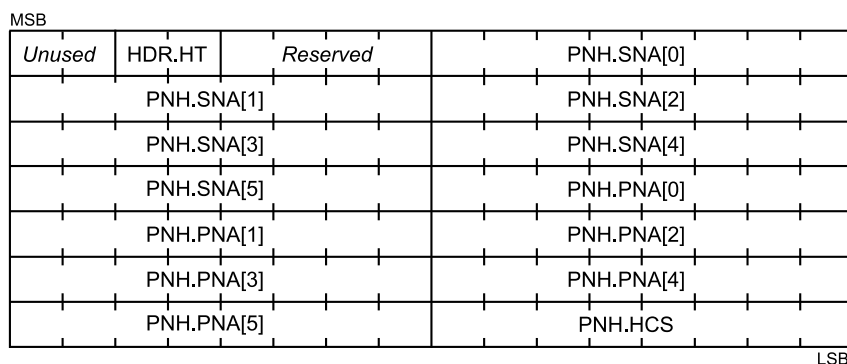
4.4.2.4 KONTROLA CRC

Kontrola CRC ostatniego pola GPDU. Ma ono długość 32 bitów. Służy do wykrywania błędów transmisji. Ta kontrola CRC powinna obejmować konkatencję SNA w jednostkami GPDU poza samym polem CRC.

Wielomian wejściowy $M(x)$ ma postać wielomianu, którego współczynniki są sprawdzanymi bitami danych (pierwszy bit do sprawdzenia jest najwyższym współczynnikiem korelacji, a ostatni bit do sprawdzenia jest współczynnikiem korelacji zerowej. Wielomian generujący dla CRC wynosi $G(x)=x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^5+x^4+x^2+x+1$. Reszta $R(x)$ jest obliczona jako reszta z dzielenia $M(x) \cdot x^{32}$ przez $G(x)$. Współczynniki reszty będą następnie wyników kontrolą CRC.

4.4.3 Wymagana do promocji jednostka PDU

Jeśli węzeł jest odłączony i nie ma łączności z innymi istniejącymi węzłami przełączającymi, powinien wysłać powiadomienie do swoich sąsiadów w celu wskazania potrzeby promocji dostępnych węzłów terminala. Rys. 39 reprezentuje Wymaganą do promocji jednostkę PDU (PNPDU), która w tej sytuacji musi być nieregularnie wysyłana.



Rys. 39 - PDU MAC wymagana do promocji

Tabela 11 pokazuje pola PDU MAC wymagane do promocji.

1708

Tabela 11 - PDU MAC wymagana do promocji

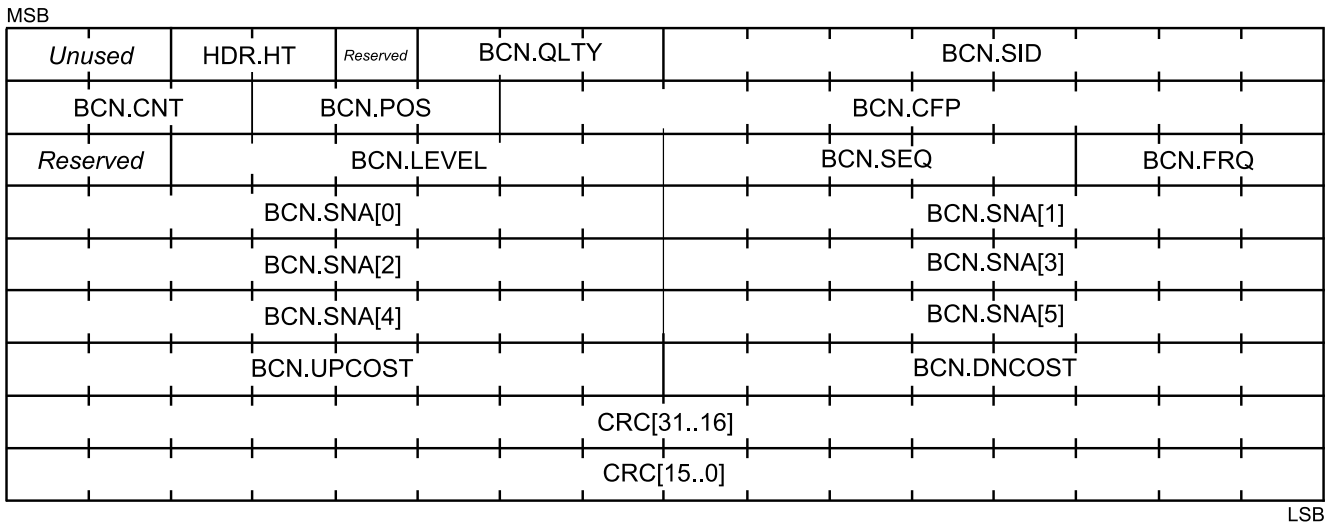
Nazwa	Długość	Opis
<i>Unused</i>	2 bity	Niewykorzystane bity, które zawsze wynoszą 0; ujęte do wyrównania z polem MAC_H w nagłówku PPDU (Punkt 3.3.3).
HDR.HT	2 bity	Typ nagłówka HDR.HT = 1 dla PDU MAC wymaganego do promocji
<i>Reserved</i>	4 bity	Zawsze 0 dla tej wersji specyfikacji. Zarezerwowany do użytku w przyszłości.
PNH.SNA	48 bitów	Adres podsieci. EUI-48 węzła podstawowego podsieci, do której połączyć próbuje się węzeł serwisowy. FF:FF:FF:FF:FF:FF, aby poprosić o promocję w dowolnej dostępnej podsieci. SNA[0] jest najbardziej znaczącym bajtem OUI/IAB, a SNA[5] jest najmniej znaczącym bajtem identyfikatora rozszerzenia, zgodnie z: http://standards.ieee.org/regauth/oui/tutorials/EUI-48.html . Powyższy zapis ma zastosowanie do wszystkich pól EUI-48 w specyfikacji.
PNH.PNA	48 bitów	Adres wymagany do promocji. EUI-48 Węzła, które wymaga promocji. Jest to EUI-48 nadajnika.
PNH.HCS	8 bitów	Sekwencja Kontrolna Nagłówka. Pole do wykrywania błędów w nagłówku. Nadajnik powinien obliczyć PNH.HCS pierwszych 13 bajtów nagłówka i wstawić wynik w pole PNH.HCS (ostatni bajt nagłówka). PNH.HCS należy obliczyć jako pozostałość z dzielenia (Modulo 2) wielomianu $M(x)=x^8+x$ przez wielomian generujący $g(x)=x^8+x^2+x+1$. $M(x)$ jest wielomianem wejściowym, który jest utworzony przez ciąg bitów nagłówka wraz z polem PNH.HCS, a najbardziej znaczący bit z ciągu bitów jest współczynnikiem najwyższego rzędu $M(x)$.

1709

1710 Ponieważ nagłówek ten jest zawsze wysyłany przez węzły niesynchronizowane, a zatem jest skłonny do
 1711 tworzenia kolizji, jest to specjalny nagłówek o zmniejszonym rozmiarze. Jest on transmitowany do innych
 1712 węzłów Terminala i dlatego powinien być przekazywany za pomocą najbardziej odpornego schematu
 1713 warstwy PHY.

1714 4.4.4 PDU sygnału

1715 Jednostka PDU sygnału (BPDU) przesyłana jest przez każde urządzenie przełączające w podsieci, w tym
 1716 węzeł podstawowy. Celem PDU jest rozpowszechnianie informacji na temat struktury ramki MAC i tym
 1717 samym dostęp kanałowy do wszystkich urządzeń, które są częścią tej podsieci. Jednostka BPDU jest
 1718 przesyłana w określonych odstępach czasu i jest również stosowana jako mechanizm synchronizujący przez
 1719 Węzły serwisowe. Rys. 40 poniżej pokazuje treść sygnału przesyłanego przez węzeł podstawowy do każdego
 1720 urządzenia przełączającego.



Rys. 40 – Struktura PDU sygnału

Tabela 12 pokazuje pola PDU sygnału.

Tabela 12 - Pola PDU sygnału

Nazwa	Długość	Opis
Unused	2 bity	Niewykorzystane bity, które zawsze wynoszą 0; ujęte do wyrównania z polem MAC_H w nagłówku PPDU (Rys. 7, punkt 3.3.3).
HDR.HT	2 bity	Typ nagłówka HDR.HT = 2 dla PDU sygnału
Reserved	1 bit	Zawsze 0 dla tej wersji specyfikacji. Zarezerwowany do użytku w przyszłości.
BCN.QLTY	3 bity	Jakość łączności określonej z węzła przełączającego do węzła podstawowego. BCN.QLTY=7 dla najlepszej jakości (Węzeł podstawowy lub bardzo dobry węzeł serwisowy), BCN.QLTY=0 dla najgorszej jakości (Węzeł przełączający z niestabilnym połączeniem z podsięcią).
BCN.SID	8 bitów	Identyfikator przełączenia transmitującego
BCN.CNT	3 bity	Liczba szczelin sygnału w tej ramce
BCN.SLT	3 bity	Szczelina sygnału, w którym wysyłany jest BPDU BCN.SLT=0 jest zastrzeżony dla węzła podstawowego
BCN.CFP	10 bitów	Wyrównanie okresu CFP od początku ramki BCN.CFP=0 wskazuje brak CFP w ramce.
Reserved	1 bit	Zawsze 0 dla tej wersji specyfikacji. Zarezerwowany do użytku w przyszłości.
BCN.LEVEL	6 bitów	Hierarchia przesyłania przełączenia w podsięci

Nazwa	Długość	Opis
BCN.SEQ	5 bitów	Liczba sekwencji dla tej BPDU w superramce. Liczba jest zwiększana dla każdego sygnału, który wysyła węzeł podstawowy i jest propagowana przez Przełączenie przez jej jednostkę BPDU, tak że cała podsieć ma w danym momencie tę samą liczbę sekwencji.
BCN.FRQ	3 bity	Częstotliwość transmisji tej jednostki BPDU. Wartości te zinterpretowano następująco: 0 = 1 sygnał co 1 ramka 1 = 1 sygnał co 2 ramki 2 = 1 sygnał co 4 ramki 3 = 1 sygnał co 8 ramek 4 = 1 sygnał co 16 ramek 5 = 1 sygnał co 32 ramki 6 = Zarezerwowany 7 = Zarezerwowany
BCN.SNA	48 bitów	Identyfikator podsieci, w której znajduje się przełączenie wysyłające BPDU.
BCN.UPCOST	8 bitów	Całkowity koszt łącza ładowania z przesyłającego węzła przełączającego do węzła podstawowego. Koszt jednego hopu jest obliczany na podstawie systemu modulacji w tym hopie w kierunku łącza ładowania. Wartości zostały określone w następujący sposób: 8PSK = 0 QPSK = 1 BPSK = 2 8PSK_F = 1 QPSK_F = 2 BPSK_F 4 Węzeł podstawowy przekaże w swoim sygnale BCN.UPCOST = 0. Węzeł przełączający prześle swoim sygnale wartość BCN.UPCOST odebraną ze swojego węzła przełączającego wyżej w hierarchii wraz z kosztem hopu łącza ładowania do jego węzła przełączającego. Gdy wartość ta jest większa niż wartość, jaka może się zmieścić w BCN.UPCOST, należy zastosować maksymalną wartość BCN.UPCOST.

Nazwa	Długość	Opis
BCN.DNCOST	8 bitów	Całkowity koszt połączenia pobierającego z węzła podstawowego do przesyłającego węzła przełączającego. Koszt jednego hopu jest obliczany na podstawie systemu modulacji w tym hopie w kierunku połączenia pobierającego. Wartości zostały określone w następujący sposób: 8PSK 0 QPSK 1 BPSK 2 8PSK_F 1 QPSK_F 2 BPSK_F 4 Węzeł podstawowy przekaże w swoim sygnale BCN.DNCOST = 0. Węzeł przełączający prześle swoim sygnale wartość BCN.DNCOST odebraną ze swojego węzła przełączającego wyżej w hierarchii wraz z kosztem hopu połączenia pobierającego z jego węzła przełączającego. Gdy wartość ta jest większa niż wartość, jaka może się zmieścić w BCN.DNCOST, należy zastosować maksymalną wartość BCN.DNCOST.
CRC	32 bity	Kontrolę CRC należy obliczyć z tym samym algorytmem, jako kontrolę zdefiniowaną dla pola CRC jednostki PDU MAC (patrz punkt 4.4.2.4). Tą kontrolę CRC można obliczyć w pełnych jednostkach BPDU poza samym polem CRC.

1725

1726 Jednostka BPDU jest również stosowana do wykrywania, przełączenie łącza ładowania nie jest już dostępne
 1727 z powodu zmiany charakterystyk medium lub z powodu błędu, itd. Jeśli węzeł serwisowy nie odbierze $N_{\text{miss-beacon}}$
 1728 sygnatów w rzędzie, zdeklaruje on łącze do swojego przełączenia jako nieużyteczne. Węzeł serwisowy
 1729 powinien zaprzestać wysyłania sygnatów, jeśli działa on jako przełączenie. Powinien on zamknąć wszystkie
 1730 istniejące połączenia MAC. Węzeł serwisowy następnie wprowadzi wstępny niezarejestrowany stan
 1731 funkcjonalny i wyszukuje dołączenie do podsieci. Ten mechanizm uzupełnia mechanizm utrzymywania
 1732 aktywności Keep-Alive stosowany przez węzeł podstawowy i jego przełączenia do określania czasu utraty
 1733 węzła serwisowego.

1734 4.4.5 Pakiety kontrolne MAC

1735 4.4.5.1 Ogólne

1736 Pakiety kontrolne MAC umożliwiają węzłowi serwisowemu przekazywanie informacji kontrolnych z węzłem
 1737 przełączającym, węzłem podstawowym i vice versa. Pakiet kontrolny przesyłany jest jako GPDU i
 1738 identyfikowany za pomocą bitu PKT.C ustawionego na 1 (patrz punkt 4.4.2, aby uzyskać więcej informacji na
 1739 temat pól pakietów).

1740 Istnieje kilka typów komunikatów kontrolnych. Każdy rodzaj komunikatu kontrolnego jest identyfikowany
 1741 przez pole PKT.CTYPE. Tabela 13 pokazuje typy komunikatów kontrolnych. Treść pakietu (patrz punkt

1742 4.4.2.3) powinna zawierać informacje przenoszone przez pakiety kontrolne. Informacje te różnią się w
1743 zależności od typu pakietu.

1744 Tabela 13 - Typy pakietu kontrolnego MAC

Typ (PKT.CTYPE)	Nazwa pakietu	Opis pakietu
1	REG	Zarządzanie rejestracją
2	CON	Zarządzanie połączeniami
3	PRO	Zarządzanie promocją
4	BSI	Informacje na temat szczeliny sygnału
5	FRA	Zmiana struktury ramki
6	CFP	Żądanie okresu współdzielonej kontencji
7	ALV	Utrzymanie aktywności
8	MUL	Zarządzanie Multicast
9	PRM	Zarządzanie odpornością warstwy PHY
10	SEC	Informacje o zabezpieczeniach

1745

1746 4.4.5.2 Retransmisja pakietu kontrolnego

1747 Dla odzyskiwania danych z utraconych komunikatów kontrolnych określa się schemat retransmisji. Po
1748 mechanizmie retransmisji, opisanym w niniejszym punkcie, nastąpić mogą transakcje kontrolne MAC
1749 polegające na wymianie jednego lub większej liczby pakietów kontrolnych.

1750 Schemat retransmisji powinien być stosowany do następujących pakietów, gdy wymagają one odpowiedzi:

- 1751 • CON_REQ_S, CON_REQ_B;
- 1752 • CON_CLS_S, CON_CLS_B;
- 1753 • REG_RSP;
- 1754 • PRO_REQ_B;
- 1755 • BSI_IND;
- 1756 • MUL_JOIN_S, MUL_JOIN_B;
- 1757 • MUL_LEAVE_S, MUL_LEAVE_B;

1758 Urządzenia biorące udział w transakcji kontrolnej MAC korzystające z mechanizmu retransmisji liczą ile razy
1759 komunikat został retransmitowany i zarządzają zegarem retransmisji.

1760 U wysyłającego żądanie transakcji komunikatu kontrolnego:

- 1761 • Gdy przesyłany jest pierwszy komunikat w transakcji, zegar retransmisji uruchamiany jest z
1762 wartością *macCtReTxTimer*, a liczba retransmisji jest zerowana.

1763 Jeśli odebrany zostanie komunikat odpowiedzi, zegar retransmisji zostanie zatrzymany, a transakcja
 1764 zostanie uznana za zakończoną. Należy zauważyć, że możliwe jest dalsze odbieranie komunikatów
 1765 odpowiedzi. Byłyby to komunikaty, które natrafiły na opóźnienia w sieci.

1766 • Jeżeli czas retransmisji upłynie, licznik retransmisji jest zwiększany. Jeśli licznik retransmisji jest
 1767 mniejszy niż *macMaxCt/ReTx*, komunikat kontrolny jest retransmitowany. Jeśli licznik jest równy
 1768 maksymalnej liczbie retransmisji, wynik niepowodzenia odpowiadający odpowiedniemu SAP MAC
 1769 powinien zostać zwrócony do jednostki wywołującej. Implementacja może również informować
 1770 lokalną jednostkę zarządzającą o takim niepowodzeniu. Jeśli retransmisja jest wykonywana przez
 1771 Węzeł serwisowy, urządzenie powinno powrócić do stanu *Rozłączony*.

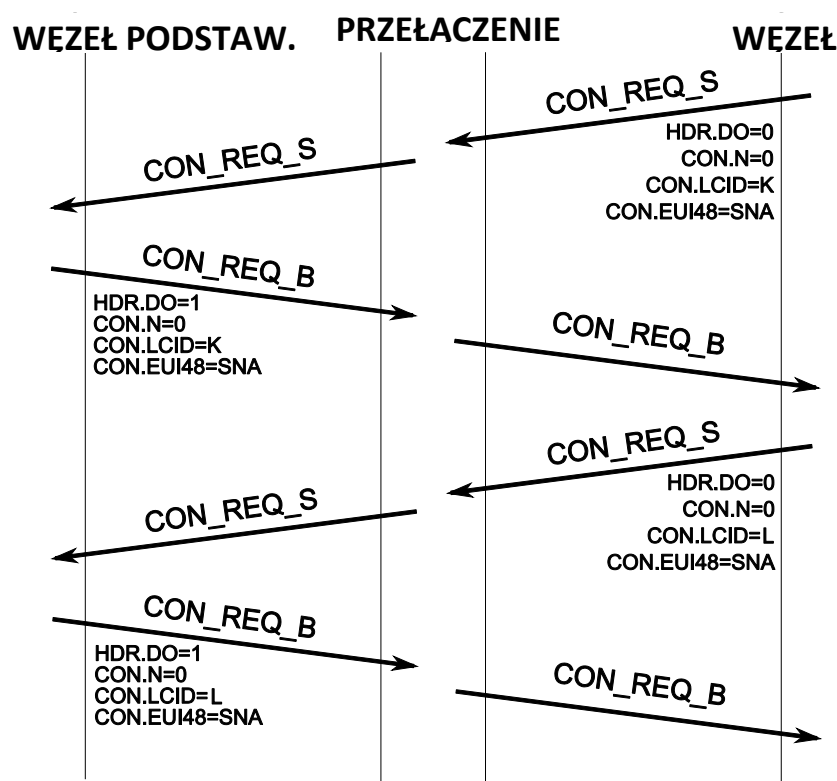
1772 U odpowiadającego na żądanie transakcji komunikatu kontrolnego:

1773 • Odbiorca komunikatu musi określić się, czy ten komunikat jest retransmisją. Jeśli tak jest, nie są
 1774 potrzebne inne żadne działania lokalne niż wysłanie odpowiedzi na odpowiedź.

1775 Jeśli odebrana wiadomość nie jest retransmisją, wiadomości powinny zostać przetworzone, a odpowiedź
 1776 zwrócona do nadawcy.

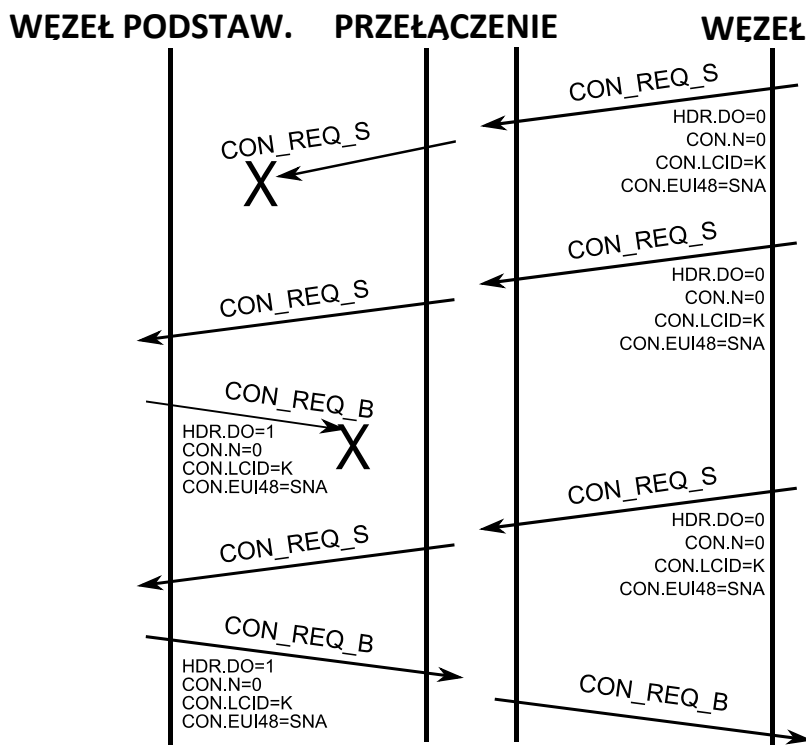
1777 • Dla transakcji, która wykorzystuje w transmisji trzy komunikaty, np. w promocji, jak pokazano w
 1778 punkcie 4.6.3, respondent powinien wykonać retransmisję w sposób identyczny jak żądający.
 1779 Gwarantuje to, że jeżeli trzeci komunikat w transakcji zostanie utracony, komunikat zostanie
 1780 ponowiony, a transakcja zakończona.

1781 Poniższe wykresy sekwencji komunikatów pokazują kilka przykładów retransmisji. Rys. 41 pokazuje dwie
 1782 udane transakcje niewymagające retransmisji.



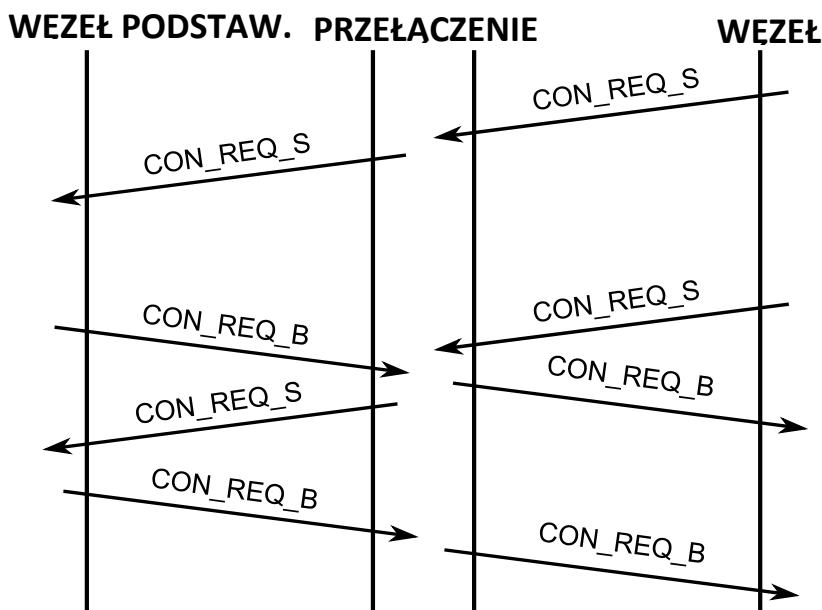
Rys. 41 – Dwie transakcje niewymagające retransmisji

1785 Rys. 42 pokazuje bardziej złożony przykład, w którym komunikaty są gubione w obu kierunkach, co
 1786 prowadzi do wielu retransmisji przed ukończeniem transakcji.



Rys. 42 - Transakcja ze stratą pakietów wymagająca retransmisji

1789 Rys. 43 pokazuje przypadek opóźnionej odpowiedzi powodującej duplikowanie w inicjatorze transakcji
 1790 kontrolnych.



Rys. 43 – Wykrywanie i eliminowanie duplikatów pakietów

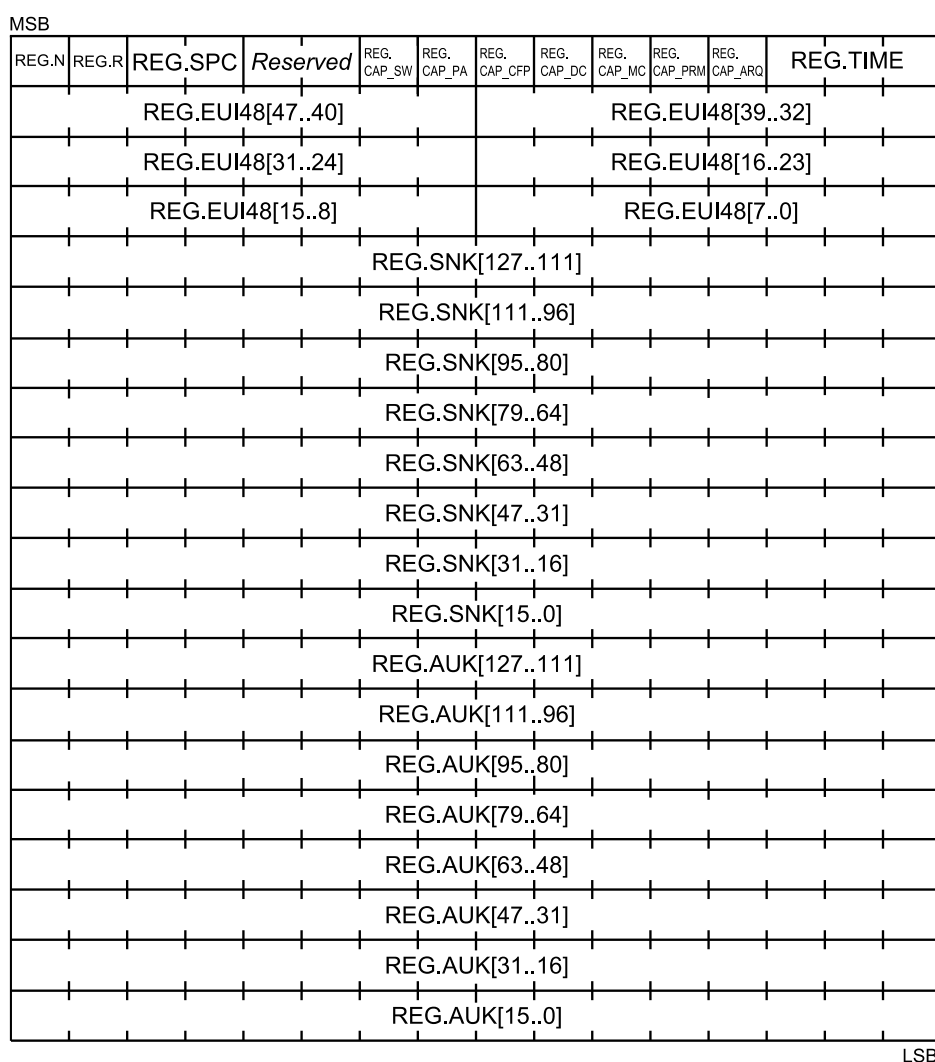
1793 4.4.5.3 Pakiet kontrolny REG (PKT.CTYPE=1)

1794 Ten pakiet kontrolny stosowany jest do negocjowania procesu rejestracji. Opis pól danych w tym pakiecie
 1795 kontrolnym opisano w Tabeli 14 oraz na Rys. 44. Znaczenie pakietów może różnić się w zależności od

1796 kierunku pakietu. Interpretację tego pakietu opisano w Tabeli 15. Pakiety te są używane w czasie procesów
 1797 rejestracji i wyrejestrowywania jak wyjaśniono w punktach 4.6.1 i 4.6.2.

1798 Pole PKT.SID jest używana w tym pakiecie kontrolnym jako przełączenie, w którym zarejestrowany jest
 1799 węzeł serwisowy. Pole PKT.SID jest używana w tym pakiecie kontrolnym jako identyfikator węzła lokalnego
 1800 przypisywany do węzła serwisowego w czasie negocjowania procesu rejestracji.

1801 Pole REG.CAP_PA jest używane do wskazania uprawnienia do agregacji pakietu, jak omówiono w punkcie
 1802 4.3.7. W kierunku łącza ładowania pole to jest wskazaniem uprawnień rejestrującego węzła terminala. Dla
 1803 odpowiedzi połączenia pobierającego węzeł podstawowy ocenia czy wszystkie urządzenia w kaskadowym
 1804 łańcuchu od węzła podstawowego do węzła terminal posiadają uprawnienie do agregacji pakietów czy nie.
 1805 Jeśli tak jest, węzeł podstawowy powinien ustawić REG.CAP_PA=1; w przeciwnym razie REG.CAP_PA=0.



1806

1807

Rys. 44 - Struktura pakietu kontrolnego REG

1808

Tabela 14 - Pola pakietu kontrolnego REG

Nazwa	Długość	Opis
REG.N	1 bit	Ujemny - REG.N=1 dla rejestru ujemnego; - REG.N=0 dla rejestru dodatniego. (patrz Tabela 15)
REG.R	1 bit	Roaming - REG.R=1 jeśli węzeł jest już zarejestrowany i chce wykonać roaming do innego przełączenia; - REG.R=0 jeśli węzeł nie jest jeszcze zarejestrowany i chce wykonać „czysty” proces rejestracji.
REG.SPC	2 bity	Profil zabezpieczeń możliwy dla PDU danych: - REG.SPC=0 Szyfrowanie niemożliwe; - Urządzenie o możliwym Profilu bezpieczeństwa 1 REG.SPC=1; - Urządzenie o możliwym Profilu bezpieczeństwa 2 REG.SPC=2 (jeszcze nieokreślone); - Urządzenie o możliwym Profilu bezpieczeństwa 3 REG.SPC=3 (jeszcze nieokreślone).
<i>Reserved</i>	2 bity	Zarezerwowany dla przyszłych wersji protokołu. Powinien być ustawiony na 0 dla tej wersji protokołu.
REG.CAP_SW	1 bit	Możliwe przełączenie 1 jeśli urządzenie potrafi zachowywać się jak węzeł przełączający; 0 jeśli urządzenie tego nie potrafi.
REG.CAP_PA	1 bit	Agregacja pakietów możliwa 1 jeśli urządzenie posiada możliwość agregacji pakietów (łączy ładowania) jeśli ścieżka transportu danych do urządzenia posiada możliwość agregacji pakietów (Połączenie pobierające) 0 w innym razie.
REG.CAP_CFP	1 bit	Okres bezkolizyjnego dostępu możliwy 1 jeśli urządzenie może przeprowadzić negocjacje CFP; 0 jeśli urządzenie nie może używać Okresu bezkolizyjnego dostępu w wynegocjowany sposób.

Nazwa	Długość	Opis
REG.CAP_DC	1 bit	Połączenie bezpośrednie możliwe 1 jeśli urządzenie może wykonać połączenia bezpośrednie; 0 jeśli urządzenie nie może wykonać połączeń bezpośrednich.
REG.CAP_MC	1 bit	Multicast możliwy 1 jeśli urządzenie może wykorzystać multicast do własnej komunikacji; 0 jeśli urządzenie nie może wykorzystać multicast do własnej komunikacji.
REG.CAP_PRM	1 bit	Zarządzanie odpornością warstwy PHY możliwe 1 jeśli urządzenie może przeprowadzić Zarządzanie odpornością warstwy PHY; 0 jeśli urządzenie nie może przeprowadzić Zarządzania odpornością warstwy PHY.
REG.CAP_ARQ	1 bit	ARQ możliwe 1 jeśli urządzenie może ustanowić połączenia ARQ; 0 jeśli urządzenie nie może ustanowić połączeń ARQ.
REG.TIME	3 bity	Czas oczekiwania na komunikaty ALV_B przy założeniu, że Węzeł serwisowy został zarejestrowany przez Węzeł podstawowy. Dla wszystkich komunikatów poza REG_RSP to pole powinno być ustawione na 0. Dla REG_RSP wartość wynosi: ALV.TIME = 0 => 32 sekund; ALV.TIME = 1 => 64 sekund; ALV.TIME = 2 => 128 sekund ~ 2,1 minuty; ALV.TIME = 3 => 256 sekund ~ 4,2 minuty; ALV.TIME = 4 => 512 sekund ~ 8,5 minuty; ALV.TIME = 5 => 1024 sekund ~ 17,1 minuty; ALV.TIME = 6 => 2048 sekund ~ 34,1 minuty; ALV.TIME = 7 => 4096 sekund ~ 68,3 minuty.
REG.EUI-48	48 bitów	EUI-48 Węzła EUI-48 węzła wysyła żądanie rejestracji.
REG.SNK	128 bitów	Zaszyfrowany klucz podsieci, które jest stosowany do wyprowadzania klucza roboczego podsieci.
REG.AUK	128 bitów	Zaszyfrowany klucz uwierzytelniający. Jest to losowy ciąg przeznaczony do działania jako mechanizm uwierzytelniania.

1809

Tabela 15 - Typy pakietu kontrolnego REG

Nazwa	HDR.DO	PKT.LNID	REG.N	REG.R	Opis
REG_REQ	0	0x3FFF	0	R	Żądanie rejestracji - Jeśli R=0, wszystkie poprzednie połączenia z tego węzła powinny zostać utracone; - Jeśli R=1, wszystkie poprzednie połączenia z tego węzła powinny zostać utrzymane.
REG_RSP	1	< 0x3FFF	0	R	Odpowiedź rejestracji. Ten pakiet przypisuje PCK.LNID do węzła serwisowego.
REG_ACK	0	< 0x3FFF	0	R	Rejestracja zatwierdzona przez Węzeł serwisowy.
REG_REJ	1	0x3FFF	1	0	Rejestracja odrzucona przez węzeł podstawowy.
REG_UNR_S	0	< 0x3FFF	1	0	- Po REG_UNR_B: Potwierdzenie wyrejestrowania; - Samodzielnie: Żądanie wyrejestrowania rozpoczęte przez Węzeł.
REG_UNR_B	1	< 0x3FFF	1	0	- Po REG_UNR_S: Potwierdzenie wyrejestrowania; - Samodzielnie: Żądanie wyrejestrowania rozpoczęte przez Węzeł podstawowy.

1810

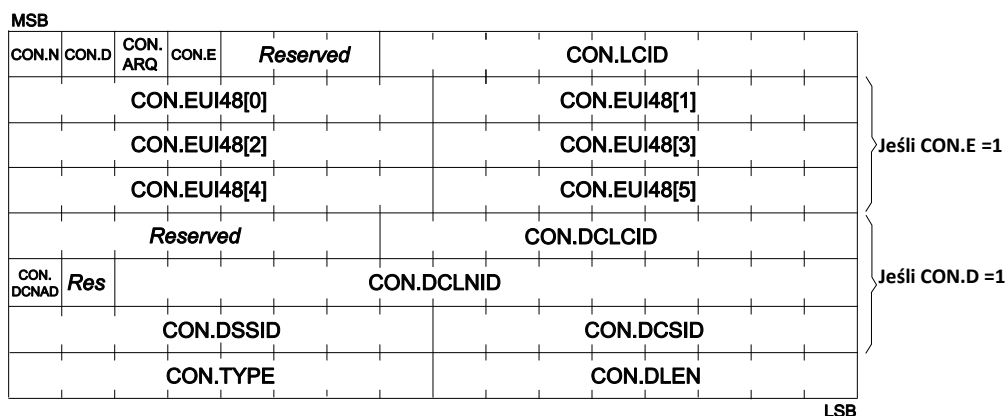
1811 Pola REG.SNK and REG.AUK są prawidłowe jedynie dla komunikatów REG_RSP i REG_ACK z Profilem
 1812 Zabezpieczeń 1 (REG.SCP=1). Dla wszystkich innych wariantów wymiany komunikatów za pomocą pakietu
 1813 kontrolnego REG, te pola nie powinny występować, tym samym ograniczając długość treści.

1814 W komunikacie REG_RSP „REG.SNK” oraz „REG.AUK” zawsze należy umieszczać zaszyfrowane za pomocą
 1815 WK0.

1816 W komunikacie REG_ACK pole REG.SNK jest ustawione na zero. Zawartość pola REG.AUK powinna zostać
 1817 wyprowadzona poprzez rozszyfrowanie odebranej wiadomości REG_RSP z WK0 i ponowne zaszyfrowanie
 1818 rozszyfrowanego pola REG.AUK z SWK wyprowadzonym z rozszyfrowanej wiadomości REG.SNK i losowego
 1819 ciągu poprzednio odebranego w pakietach kontrolnych SEC.

1820 4.4.5.4 Pakiet kontrolny CON (PKT.CTYPE = 2)

1821 Ten pakiet kontrolny stosowany jest do negocjowania połączeń. Opis pól tego pakietu podano w Tabela 16 i
 1822 na Rys. 45 Znaczenie pakietów może różnić się w zależności od kierunku pakietu i wartości różnych typów.
 1823 Tabela 17 pokazuje różne interpretacje pakietów. Pakiety są używane podczas nawiązywania i zamykania
 1824 połączenia. Procesy te wyjaśniono bardziej szczegółowo w punkcie 4.6.6.



Rys. 45 - Struktura pakietu kontrolnego CON

Należy zauważyć, że Rys. 45 pokazuje cały komunikat wraz z wszystkimi opcjonalnymi elementami. Gdy CON.D wynosi 0, CON.DCNAD, CON.DSSID, CON.DCLNID, CON.DCLCID, CON.DCSID i zarezerwowane pole pomiędzy CON.DCNAD i CON.DSSID nie będą występować w tej wiadomości. Tym samym komunikat będzie o 6 oktetów mniejszy. Podobnie, gdy CON.E wynosi zero, pole CON.EUI-48 nie będzie występować, przez co komunikat będzie o 6 oktetów krótszy.

Tabela 16 - Pola pakietu kontrolnego CON

Nazwa	Długość	Opis
CON.N	1 bit	Ujemny - CON.N=1 dla połączenia ujemnego; - CON.N=0 dla połączenia dodatniego.
CON.D	1 bit	Połączenie bezpośrednie - CON.D=1 jeśli informacje o bezpośrednim połączeniu są realizowane przez ten pakiet; - CON.D=0 jeśli informacje o bezpośrednim połączeniu nie są realizowane przez ten pakiet.
CON.ARQ	1 bit	Mechanizm ARQ włączony - CON.ARQ=1 jeśli mechanizm ARQ jest włączony dla tego połączenia. - CON.ARQ=0 jeśli mechanizm ARQ nie jest włączony dla tego połączenia.
CON.E	1 bit	Obecność EUI-48 - CON.E = 1, aby uzyskać CON.EUI-48; - CON.E = 0, aby nie mieć CON.EUI-48, więc ustanawianie tego połączenia służy do uzyskania warstwy konwergencji węzła podstawowego.

Nazwa	Długość	Opis
<i>Reserved</i>	3 bity	Zarezerwowany dla przyszłych wersji protokołu. Powinno być to 0 dla tej wersji protokołu.
CON.LCID	9 bitów	Identyfikator Połączenia Lokalnego. LCID jest zarezerwowany w żądaniu połączenia. Identyfikatory LCID od 0 do 255 są przypisane przez żądania połączenia rozpoczęte przez Węzeł podstawowy. Identyfikatory LCID od 256 do 511 są przypisane przez żądania połączenia rozpoczęte przez węzeł lokalny. Jest to identyfikator połączenia zarządzanego za pomocą tego pakietu. Nie jest one taki sam jak PKT.LCID ogólnego nagłówka, który nie istnieje dla pakietów kontrolnych.
CON.EUI-48	48 bitów (Obecny CON.E=1)	jeśli EUI-48 docelowego/źródłowego węzła serwisowego/węzła podstawowego dla żądania połączenia. Gdy połączenie kierunkowane nie jest przeprowadzane, pole to nie powinno być ujęte. Podczas wykonywania połączenia kierunkowanego pole może zawierać adres SNA, wskazujący, że warstwa konwergencji węzła podstawowego powinna określać EUI-48. • CON.D = 0, Docelowy EUI-48; • CON.D = 1, Źródłowy EUI-48.
<i>Reserved</i>	7 bitów (Dotyczy CON.D=1)	jeśli Zarezerwowany dla przyszłych wersji protokołu. Powinno być to 0 dla tej wersji protokołu.
CON.DCLCID	9 bitów (Dotyczy CON.D=1)	jeśli LCID połączenia bezpośredniego To pole reprezentuje identyfikator LCID połączenia, w którym już ustanowiony identyfikator powinien być bezpośrednio przełączony.
CON.DCNAD	1 bit (Dotyczy CON.D=1)	jeśli Zarezerwowany dla przyszłych wersji protokołu. Brak agregacji połączenia bezpośredniego w miejscu docelowym To pole określa treść pola PKT.NAD po działaniu bezpośredniego przełączenia połączenia.
<i>Reserved</i>	1 bit (Dotyczy CON.D=1)	jeśli Zarezerwowany dla przyszłych wersji protokołu. Powinno być to 0 dla tej wersji protokołu.

Nazwa	Długość	Opis
CON.DCLNID	14 bitów (Dotyczy CON.D=1) jeśli	LNID połączenia bezpośredniego To pole reprezentuje identyfikator LNID połączenia, w którym już ustanowiony identyfikator powinien być bezpośrednio przełączony.
CON.DSSID	8 bitów (Dotyczy CON.D=1) jeśli	SID przełączenia bezpośredniego To pole reprezentuje SID przełączenia, które powinno dowiedzieć się o połączeniu bezpośrednim i wykonać przełączanie bezpośrednie.
CON.DCSID	8 bitów (Dotyczy CON.D=1) jeśli	SID połączenia bezpośredniego To pole reprezentuje identyfikator SID połączenia, w którym już ustanowiony identyfikator powinien być bezpośrednio przełączony.
CON.TYPE	8 bitów	Typ połączenia. Typ połączenia (patrz Załącznik E) określa warstwę konwergencji do stosowania dla tego połączenia. Są one traktowane transparentnie w podwarstwie MAC wspólnej części MAC i są stosowane wyłącznie do określenia, która warstwa konwergencji ma być stosowana.
CON.DLEN	8 bitów	Długość pola CON.DATA w bajtach
CON.DATA	(zmienna)	Parametry właściwe dla połączenia. Te parametry właściwe dla połączenia są właściwe dla warstwy konwergencji. Powinny być one określone w każdej warstwie konwergencji do określania parametrów, które są właściwe dla połączenia. Parametry te są traktowane w sposób przejrzysty przez podwarstwę wspólnej części.

1833

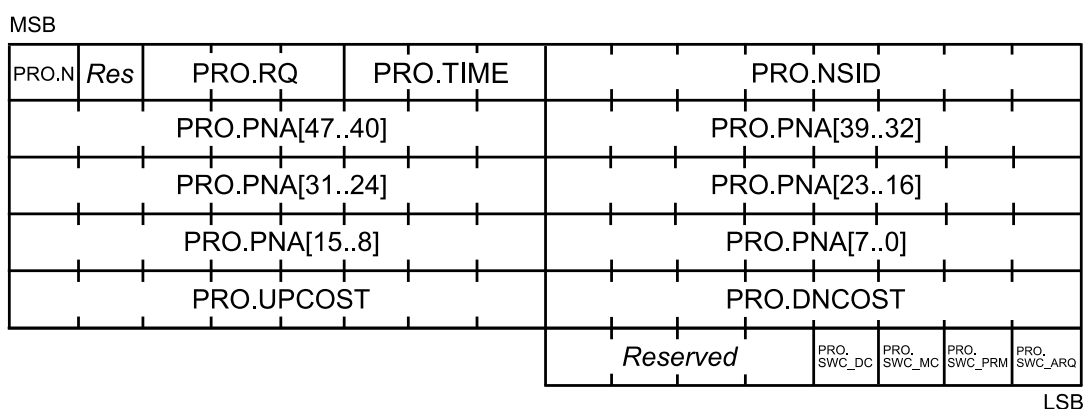
Tabela 17 - Typy pakietu kontrolnego CON

Nazwa	HDR.DO	CON.N	Opis
CON_REQ_S	0	0	Żądanie ustanowienia połączenia zainicjowanego przez węzeł serwisowy.
CON_REQ_B	1	0	Węzeł podstawowy uzna, że to połączenie jest nawiązywane z identyfikatorem CON.LCID. - Po CON_REQ_S: Połączenie zatwierdzone; - Samodzielnie: Żądanie ustanawiania połączenia.
CON_CLS_S	0	1	Węzeł serwisowy uważa, że to połączenie jest zamknięte: - Po CON_REQ_B: Połączenie odrzucone przez węzeł; - Po CON_CLS_B: Potwierdzenie zamknięcia połączenia; - Samodzielnie: Żądanie zamknięcia połączenia.

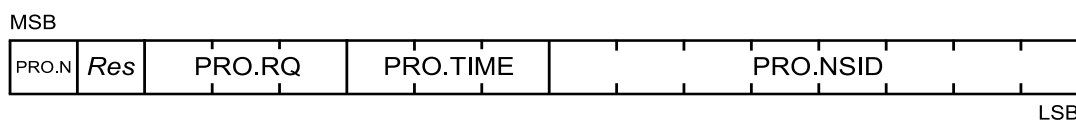
Nazwa	HDR.DO	CON.N	Opis
CON_CLS_B	1	1	Węzeł podstawowy uzna, że to połączenie nie jest już nawiązywane. - Po CON_REQ_S: Ustawianie połączenia odrzucone przez węzeł podstawowy; - Po CON_CLS_S: Potwierdzenie zamknięcia połączenia; - Samodzielnie: Żądanie zamknięcia połączenia.

1834 4.4.5.5 Pakiet kontrolny PRO (PKT.CTYPE = 3)

1835 Ten pakiet kontrolny stosowany jest do promocji węzła serwisowego z funkcji terminala do funkcji
 1836 przełączania. Opis pól tego pakietu podano w Tabela 18, na Rys. 46 oraz Rys. 47 . Znaczenie pakietów może
 1837 różnić się w zależności od kierunku pakietu i wartości różnych typów. Tabela 19 pokazuje różne
 1838 interpretacje pakietów. Proces promocji wyjaśniono bardziej szczegółowo w punkcie 4.6.3.



Rys. 46 - Struktura pakietu kontrolnego PRO_REQ_S



Rys. 47 - Struktura pakietu kontrolnego PRO

1844 Należy zauważyć, że Rys. 46 pokazuje wszystkie pola używane w komunikacie PRO_REQ_S. Wszystkie inne
 1845 komunikaty są znacznie mniejsze, zawierając tylko PRO.N, PRO.RC, PRO.TIME i PRO.NSID, jak pokazano na
 1846 Rys. 47.

Tabela 18 - Pola pakietu kontrolnego PRO

Nazwa	Długość	Opis
PRO.N	1 bit	Ujemny PRO.N=1 dla promocji ujemnej PRO.N=0 dla promocji dodatniej

Nazwa	Długość	Opis
<i>Reserved</i>	1 bit	Zarezerwowany dla przyszłych wersji protokołu Powinno być to 0 dla tej wersji protokołu.
PRO.RQ	3 bity	Jakość odbioru komunikatu PNPDU odebranego z węzła serwisowego żądającego promocji od terminala.
PRO.TIME	3 bity	Wartość ALV.TIME która jest używana przez terminal, który stanie się przełączeniem. Po odebraniu tego czasu w PRO_REQ_B, węzeł serwisowy powinien zresetować zegar utrzymywania aktywności w ten sam sposób, jak podczas odbierania ALV_B.
PRO.NSID	8 bitów	Identyfikator nowego przełączenia. Jest to przypisany identyfikator połączenia węzła, którego promocja jest zarządzana za pomocą tego pakietu. Nie jest to ten sam identyfikator PKT.SID nagłówka pakietu, który musi być identyfikatorem SID przełączenia, do którego połączony jest węzeł jako węzeł terminala.
PRO.PNA	0 lub 48 bitów	Adres wymagany do promocji zawiera EUI-48 terminala wymagającego promocji węzła serwisowego, aby stać się węzłem przełączającym. To pole zawarte jest jedynie w komunikacie PRO_REQ_S.
PRO.UPCOST	0 lub 8 bitów	Całkowity koszt łącza ładowania z węzła terminala do węzła podstawowego. Ta wartość jest obliczana w ten sam sposób, w jaki węzeł przełączający oblicza wartość umieszczaną w jedno własnej PDU sygnału. To pole zawarte jest jedynie w komunikacie PRO_REQ_S.
PRO.DNCOST	0 lub 8 bitów	Całkowity koszt połączenia pobierającego z węzła podstawowego do węzła terminala. Ta wartość jest obliczana w ten sam sposób, w jaki węzeł przełączający oblicza wartość umieszczaną w jedno własnej PDU sygnału. To pole zawarte jest jedynie w komunikacie PRO_REQ_S.
<i>Reserved</i>	4 bity	Zarezerwowany dla przyszłych wersji protokołu. Powinien być ustawiony na 0 dla tej wersji protokołu.
PRO.SWC_DC	1 bit	Przełączenie połączenia bezpośredniego możliwe 1 jeśli urządzenie potrafi zachowywać się jak przełączanie bezpośrednie w połączeniach bezpośrednich. 0 w innym razie
PRO.SWC_MC	1 bit	Przełączenie multicast możliwe. 1 jeśli urządzenie potrafi zarządzać ruchem multicast podczas zachowywania się jak przełączenie. 0 w innym razie

Nazwa	Długość	Opis
PRO.SWC_PRM	1 bit	Możliwość zarządzania odpornością warstwy PHY 1 jeśli urządzenie może przeprowadzić PRM dla węzłów terminala podczas zachowywania się jak Przełączenie. 0 jeśli urządzenie nie może przeprowadzić PRM podczas zachowywania się jak Przełączenie.
PRO.SWC_ARQ	1 bit	Przełączanie buforowania ARQ możliwe 1 jeśli urządzenie potrafi wykonać buforowanie połączeń ARQ podczas przełączania. 0 jeśli urządzenie nie może wykonać buforowania dla połączeń ARQ podczas przełączania.

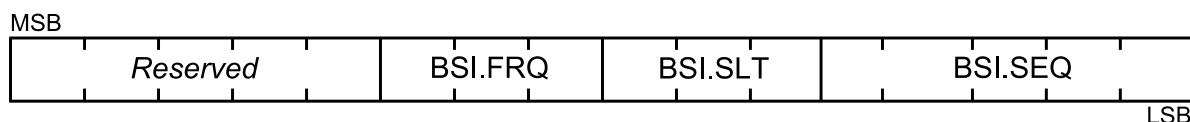
1848

Tabela 19 - Typy pakietu kontrolnego PRO

Nazwa	HDR.DO	PRO.N	PRO.NSID	Opis
PRO_REQ_S	0	0	0xFF	Żądanie promocji rozpoczęte przez Węzeł serwisowy.
PRO_REQ_B	1	0	< 0xFF	Węzeł podstawowy uzna, że węzeł serwisowy został promowany z identyfikatorem PRO.NSID. - Po PRO_REQ: Promocja zatwierdzona; - Samodzielnie: Żądanie promocji rozpoczęte przez Węzeł podstawowy.
PRO_ACK	0	0	< 0xFF	Zatwierdzenie promocji
PRO_REJ	1	1	0xFF	Węzeł podstawowy uważa, że węzeł serwisowy jest zdegradowany. Wysyłany jest po odrzuceniu go przez PRO_REQ.
PRO_DEM_S	0	1	< 0xFF	Węzeł serwisowy uważa, że jest on zdegradowany: - Po PRO_DEM_B: Degradacja zatwierdzona; - Po PRO_REQ_B: Promocja odrzucona; - Samodzielnie: Żądanie degradacji.
PRO_DEM_B	1	1	< 0xFF	Węzeł podstawowy uważa, że węzeł serwisowy jest zdegradowany: - Po PRO_DEM_S: Degradacja zatwierdzona; - Samodzielnie: Żądanie degradacji.

4.4.5.6 Pakiet kontrolny BSI (PKT.CTYPE = 4)

Pakiet kontrolny wskazania szczeliny sygnału (BSI) stosowany jest wyłącznie przez węzeł podstawowy i węzły przełączające. Stosowany jest on do wymiany informacji, które są używane przez węzeł przełączający do przesyłania swojego sygnału. Opis pól tego pakietu podano w Tabeli 20 oraz na Rys. 48. Znaczenie pakietów może różnić się w zależności od kierunku pakietu i wartości różnych typów. **Błąd! Nie można odnaleźć źródła odwołania.** pokazuje różne interpretacje pakietów. Proces promocji wyjaśniono bardziej szczegółowo w punkcie 4.6.3.



Rys. 48 - Struktura pakietu kontrolnego BSI

Tabela 20 - Pola pakietu kontrolnego BSI

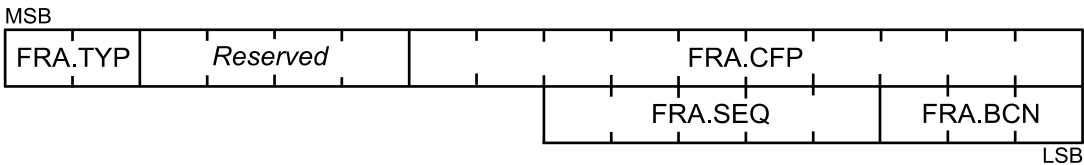
Nazwa	Długość	Opis
<i>Reserved</i>	5 bitów	Zarezerwowany dla przyszłych wersji protokołu. W tej wersji pole to powinno być inicjowane do 0.
BSI.FRQ	3 bity	Częstotliwość przesyłania szczeliny sygnału, zakodowana jako: FRQ = 0 => 1 sygnał co 1 ramka FRQ = 1 => 1 sygnał co 2 ramki FRQ = 2 => 1 sygnał co 4 ramki FRQ = 3 => 1 sygnał co 8 ramek FRQ = 4 => 1 sygnał co 16 ramek FRQ = 5 => 1 sygnał co 32 ramki FRQ = 6 => Zarezerwowana FRQ = 7 => Zarezerwowana
BSI.SLT	3 bity	Szczelina sygnału stosowana przez przełączenie docelowe
BSI.SEQ	5 bitów	Liczba sekwencji sygnału w momencie zastosowania określonej zmiany.

Tabela 21 - Typy komunikatu kontrolnego BSI

Nazwa	HDR.DO	Opis
BSI_ACK	0	Potwierdzenie odbioru komunikatu kontrolnego BSI
BSI_IND	1	Żądanie zmiany szczeliny sygnału

4.4.5.7 Pakiet kontrolny FRA (PKT.CTYPE = 5)

Ten pakiet kontrolny jest nadawany z węzła podstawowego i przekazywany przez wszystkie węzły przełączające do całej podsiaci. Jest on używany do rozpowszechniania informacji na temat zmian struktury ramki w określonym czasie w przyszłości. Opis pól tego pakietu podano w Tabeli 22, na Rys. 49. Tabela 23 pokazuje różne interpretacje pakietów.



Rys. 49 - Struktura pakietu kontrolnego FRA

Tabela 22 - Pola pakietu kontrolnego FRA

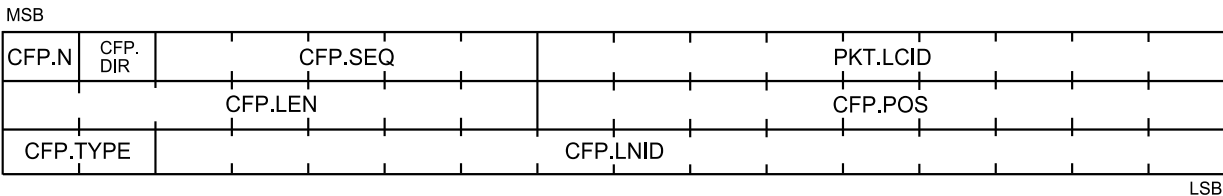
Nazwa	Długość	Opis
FRA.TYP	2 bity	0: Zmiana liczby sygnałów 1: Zmiana czasu trwania CFP
Reserved	4 bity	Zarezerwowany dla przyszłych wersji protokołu. W tej wersji pole to powinno być inicjowane do 0.
FRA.CFP	10 bitów	Wyrównanie okresu CFP od początku ramki
FRA.SEQ	5 bitów	Liczba sekwencji sygnału w momencie zastosowania określonej zmiany.
FRA.BCN	3 bity	Liczba sygnałów w ramce

Tabela 23 - Typy pakietu kontrolnego FRA

Nazwa	FRA.TYP	Opis
FRA_BCN_IND	0	Wskazuje zmiany w strukturze ramki z powodu zmian w liczbie szczelin sygnału
FRA_CFP_IND	1	Wskazuje zmiany w strukturze ramki z powodu zmian w czasie trwania CFP w wyniku przyznania CFP lub zakończenia CFP dla dowolnych węzłów serwisowych w podsięci.

4.4.5.8 Pakiet kontrolny CFP (PKT.CTYPE = 6)

Pakiet kontrolny jest używany do przydzielania dedykowanego czasu dostępu bezkolizyjnego do kanału poszczególnym węzłom terminala lub węzłom przełączającym. Opis pól tego pakietu podano w Tabela 24 oraz na **Błąd! Nie można odnaleźć źródła odwołania..** Znaczenie pakietów może różnić się w zależności od kierunku pakietu i wartości różnych typów. Tabela 25 pokazuje różne interpretacje pakietów.



Rys. 50 - Struktura pakietu kontrolnego CFP

1876

Tabela 24 - Pola komunikatu kontrolnego CFP

Nazwa	Długość	Opis
CFP.N	1 bit	0: odmowa żądania alokacji/dealokacji; 1: zatwierdzenie żądania alokacji/dealokacji.
CFP.DIR	1 bit	Wskazuje kierunek alokacji. 0: alokacja stosowana jest do łącza ładowania (w kierunku węzła podstawowego); 1: alokacja stosowana jest do Połączenia pobierającego (w kierunku węzła serwisowego).
CFP.SEQ	5 bitów	Liczba sekwencji sygnału w momencie zastosowania określonej zmiany.
CFP.LCID	9 bitów	LCID żądanego połączenia.
CFP.LEN	7 bitów	Długość (w symbolach) żądanego/przydzielonego czasu kanału na ramkę.
CFP.POS	9 bitów	Wyrównanie (w symbolach) czasu przydzielonego od początku ramki.
CFP.TYPE	2 bity	0: Pakiet alokacji kanału; 1: Pakiet dealokacji kanału; 2: Pakiet zmiany kanału.
CFP.LNID	14 bitów	LNID węzła serwisowego, który jest planowanym użytkownikiem przydziału.

1877

Tabela 25 - Typy pakietu kontrolnego CFP

Nazwa	CFP.TYP	HDR.DO	Opis
CFP_ALC_REQ_S	0	0	Węzeł serwisowy dokonuje żądania alokacji kanału
CFP_ALC_IND	0	1	- Po CFP_ALC_REQ_S: Żądany kanał jest przydzielony - Samodzielnie: Nieprzewidziana alokacja kanału przez węzeł podstawowy.
CFP_ALC_REJ	0	1	Alokacja żądanego kanału została odrzucona
CFP_DALC_REQ	1	0	Węzeł serwisowy dokonuje żądania dealokacji kanału
CFP_DALC_RSP	1	1	Węzeł podstawowy potwierdza dealokację
CFP_CHG_IND	2	1	Zmiana lokalizacji przypisanego kanału w CFP.

1878

4.4.5.9 Pakiet kontrolny ALV (PKT.CTYPE = 7)

1879

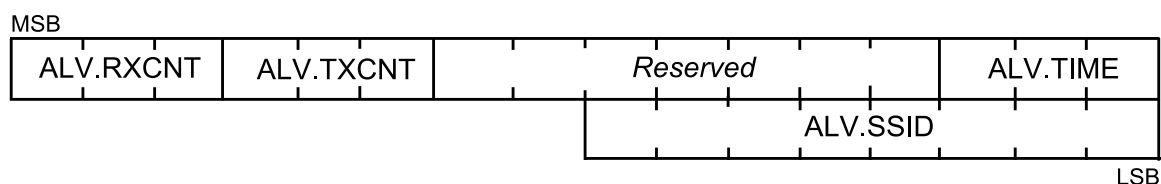
1880

1881

Komunikat kontrolny ALV jest stosowany do sygnalizowania utrzymywania aktywności pomiędzy węzłem serwisowym, węzłami serwisowym nad nimi oraz węzłem podstawowym. Wymiana komunikatów jest dwukierunkowa, to jest komunikat jest okresowo wymieniany w obu kierunkach. Strukturę tych

1882 komunikatów pokazano na **Błąd! Nie można odnaleźć źródła odwołania.** i w Tabela 26. Różne typy
 1883 komunikatu utrzymania aktywności Keep-Alive pokazano w Tabela 27. Te komunikaty są wysyłane
 1884 okresowo, jak opisano w punkcie 4.6.5.

1885



1886

1887

Rys. 51 - Struktura pakietu kontrolnego ALV

1888

1889

Tabela 26 - Pola komunikatu kontrolnego ALV

Nazwa	Długość	Opis
ALV.RXCNT	3 bity	Licznik modulo 8 do wskazywania liczby odebranych komunikatów ALV.
ALV.TXCNT	3 bity	Licznik Modulo 8 wskazujący liczbę przesłanych komunikatów ALV.
Reserved	7 bitów	Powinien zawsze być kodowany jako 0 dla tej wersji specyfikacji.
ALV.TIME	3 bity	Czas oczekiwania na komunikaty ALV_B przy założeniu, że Węzeł serwisowy został zarejestrowany przez Węzeł podstawowy. ALV.TIME = 0 => 32 sekund; ALV.TIME = 1 => 64 sekund; ALV.TIME = 2 => 128 sekund ~ 2,1 minuty; ALV.TIME = 3 => 256 sekund ~ 4,2 minuty; ALV.TIME = 4 => 512 sekund ~ 8,5 minuty; ALV.TIME = 5 => 1024 sekund ~ 17,1 minuty; ALV.TIME = 6 => 2048 sekund ~ 34,1 minuty; ALV.TIME = 7 => 4096 sekund ~ 68,3 minuty.
ALV.SSID	8 bitów	Dla pozycji Terminal, powinno to być 0xFF. Dla przełączenia jest to identyfikator przełączenia.

1890

1891

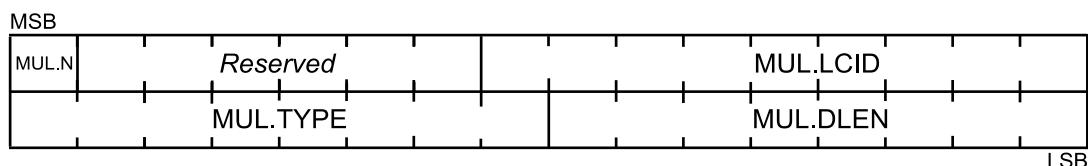
1892

Tabela 27 - Typy pakietu kontrolnego Utrzymywania aktywności

Nazwa	HDR.DO	Opis
ALV_S	0	Komunikat Utrzymania aktywności z węzła serwisowego
ALV_B	1	Komunikat utrzymywania aktywności z węzła podstawowego

1893 4.4.5.10 Pakiet kontrolny MUL (PKT.CTYPE = 8)

1894 Komunikat MUL jest używany do kontrolowania członkostwa w grupie multicast. Strukturę tego
 1895 komunikatu i znaczenia pól opisano w **Błąd! Nie można odnaleźć źródła odwołania.** i na **Błąd! Nie można**
 1896 **odnaleźć źródła odwołania..** Komunikat ten może być używany na różne sposoby, jak opisano w **Błąd! Nie**
 1897 **można odnaleźć źródła odwołania..**



Rys. 52 - Struktura pakietu kontrolnego MUL

Tabela 28 - Pola komunikatu kontrolnego MUL

Nazwa	Długość	Opis
MUL.N	1 bit	Ujemny - MUL.N = 1 dla ujemnego połączenia multicast, tj. opuszczania grupy multicast. - MUL.N = 0 dla dodatniego połączenia multicast, tj. dołączenia do grupy multicast.
Reserved	6 bitów	Zarezerwowany dla przyszłych wersji protokołu. Powinno być to 0 dla tej wersji protokołu.
MUL.LCID	9 bitów	Identyfikator Połączenia Lokalnego. LCID wskazuje, która grupa dystrybucji multicast zarządzana jest za pomocą tego komunikatu.
MUL.TYPE	8 bitów	Typ połączenia. Typ połączenia określa warstwę konwergencji do stosowania dla tego połączenia. Są one traktowane transparentnie w podwarstwie MAC wspólnej części MAC i są stosowane wyłącznie do określenia, która warstwa konwergencji ma być stosowana. Patrz Załącznik E.
MUL.DLEN	8 bitów	Długość danych w bajtach w polu MUL.DATA
MUL.DATA	(zmienna)	Parametry właściwe dla połączenia. Te parametry właściwe dla połączenia są właściwe dla warstwy konwergencji. Powinny być one określone w każdej warstwie konwergencji do określania parametrów, które są właściwe dla połączenia. Parametry te są traktowane w sposób przejrzysty przez podwarstwę wspólnej części.

1902

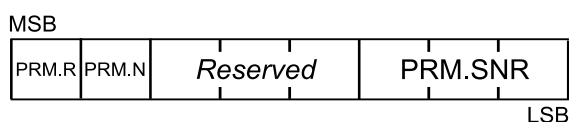
Tabela 29 - Typy komunikatu kontrolnego MUL

Nazwa	HDR.DO	MUL.N	Opis
MUL_JOIN_S	0	0	Żądanie dołączenia do grupy multicast zainicjowana przez węzeł serwisowy lub zatwierdzenie, jeśli wysłane jest w odpowiedzi na MUL_JOIN_B.
MUL_JOIN_B	1	0	Węzeł podstawowy uzna, że to połączenie dołączyło do grupy z identyfikatorem MUL.LCID. - Po MUL_JOIN_S: dołączenie zatwierdzone; - Samodzielnie: żądanie dołączenia do grupy.
MUL_LEAVE_S	0	1	Węzeł serwisowy opuszcza grupę multicast: - Po MUL_JOIN_B: Dołączenie odrzucone przez węzeł; - Po MUL_LEAVE_B: zatwierdzenie opuszczenia grupy; - Samodzielnie: żądanie opuszczenia grupy.
MUL_LEAVE_B	1	1	Węzeł podstawowy uważa, że węzeł serwisowy nie jest już członkiem grupy multicast. - Po MUL_JOIN_S: Dołączenie do grupy odrzucone przez węzeł podstawowy; - Po MUL_LEAVE_S: Zatwierdzenie opuszczenia grupy; - Samodzielnie: Żądanie opuszczenia grupy.

1903 4.4.5.11 Pakiet kontrolny PRM (PKT.CTYPE = 9)

1904 Pakiety zarządzania odpornością warstwy PHY są stosowane do kontroli parametrów, które wpływają na
 1905 odporność i skuteczność warstwy PHY. Pakiety te wysyłane są, aby powiadomić o konieczności zwiększenia
 1906 solidności transmisji lub powiadomienia, że jakość odbioru jest tak dobra, że przesłać można mniej
 1907 wytrzymały i wydajniejszy schemat modulacji.

1908 Pola pakietu kontrolnego opisano w **Błąd! Nie można odnaleźć źródła odwołania.** i na Rys. 53 a typy
 1909 komunikatów opisano w **Błąd! Nie można odnaleźć źródła odwołania.**



Rys. 53 - Struktura pakietu kontrolnego PHY

 1910
 1911

1912

1913

Tabela 30 - Pola komunikatu kontrolnego PRM

Nazwa	Długość	Opis
PRM.R	1 bit	Odpowiedź - PRM.R=1 jeśli ten komunikat jest odpowiedzią; - PRM.R=0 jeśli ten komunikat jest żądaniem.
PRM.N	1 bit	Ujemny - PRM.N=1 jeśli działania nie można wykonać. - PRM.N=0 jeśli działanie zostało przeprowadzone.
Reserved	3 bity	Powinien zawsze być kodowany jako 0 dla tej wersji specyfikacji.
PRM.SNR	3 bity	Wskazuje stosunek sygnału do szumu na końcu, który inicjuje żądanie zmiany, uzyskany za pomocą prymitywu PHY_SNR (Punkt 3.9.3.)

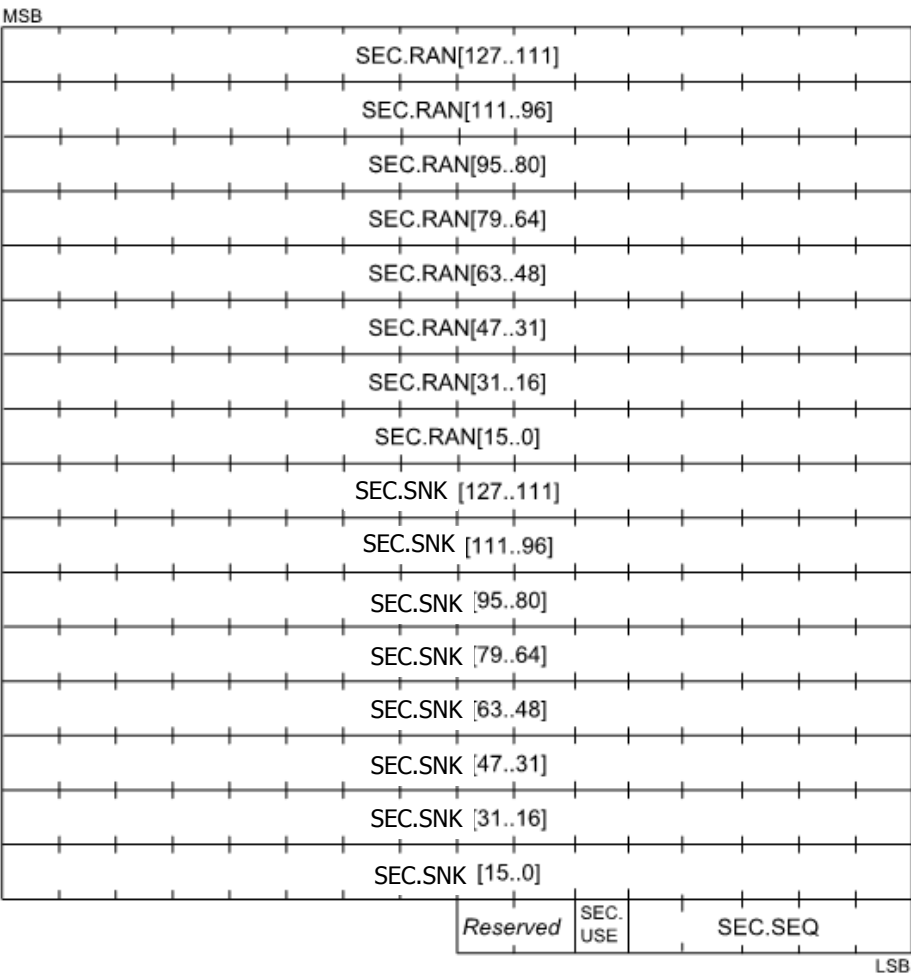
1914

Tabela 31 - Typy komunikatu kontrolnego PRM

Nazwa	PRM.R	PRM.N	Opis
PRM_REQ	0	0	Żądanie zarządzania modulacją warstwy PHY.
PRM_ACK	1	0	Zatwierdzenie zarządzania modulacją warstwy PHY.
PRM_REJ	1	1	Odrzucono zarządzanie modulacją warstwy PHY.

1915 4.4.5.12 Pakiet kontrolny SEC (PKT.CTYPE = 10)

1916 Komunikat kontrolny SEC jest nadawany jako rozszyfrowany przez węzeł podstawowy i wszystkie węzły
1917 serwisowe do pozostałej części podsięci w celu rozpowszechnienia losowej sekwencji stosowanej do
1918 generowania kluczy roboczych. Losowa sekwencja stosowana przez urządzenia w podsięci jest dynamiczna i
1919 zmienia się okresowo, aby zapewnić odporną strukturę zabezpieczeń. Strukturę tego komunikatu
1920 przedstawiono w **Błąd! Nie można odnaleźć źródła odwołania.** na Rys. 54. Szczegółowe informacje na
1921 temat mechanizmów zabezpieczeń podano w punkcie 4.3.8.



Rys. 54 - Struktura pakietu kontrolnego SEC

Tabela 32 - Pola komunikatu kontrolnego SEC

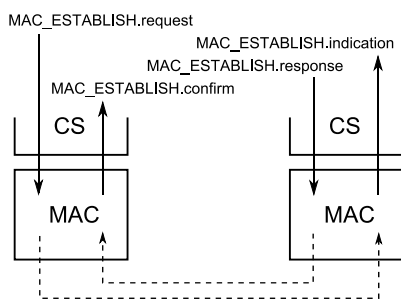
Nazwa	Długość	Opis
SEC.RAN	128 bitów	Losowy ciąg stosowany do wyprowadzenia klucza roboczego.
SEC.SNK	128 bitów	Losowy ciąg stosowany do wyprowadzenia klucza roboczego podsieci.
Reserved	2 bity	Powinien zawsze być kodowany jako 0 dla tej wersji specyfikacji.
SEC.USE	1 bit	1 wskazuje, że losowe ciągi są już w użyciu. Gdy 0 wskazuje, że SE.SEQ należy użyć do określenia kiedy rozpocząć za pomocą tych losowych sekwencji.
SEC.SEQ	5 bitów	Liczba sekwencji sygnału w momencie zastosowania określonej zmiany.

4.5 Punkt dostępu do usług MAC

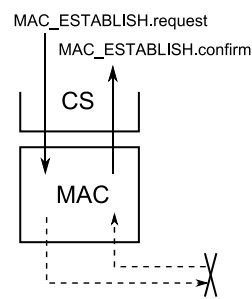
4.5.1 Ogólne

Punkt dostępu do usług MAC zapewnia kilka prymitywów umożliwiających warstwie konwergencji interakcję z warstwą MAC. Rozdział ten ma na celu wyjaśnienie sposobu stosowania warstwy MAC. Wdrożenie MAC nie może korzystać z wszystkich wymienionych tu prymitywów; może korzystać z innych prymitywów lub może posiadać interfejs oparty na połączeniu, a nie na przekazywaniu komunikatów, itd. Są to wszystko kwestie wdrożeniowe wykraczające poza zakres niniejszej specyfikacji.

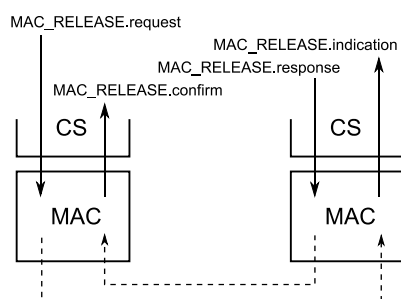
Prymityw żądania .request przekazywany jest z warstwy konwergencji do MAC w celu żądania zainicjowania usługi. Prymitywy wskazania i potwierdzenia (.indication i .confirm) przekazywane są z warstwy MAC do warstwy konwergencji w celu wskazania wewnętrznego zdarzenia MAC, które ma znaczenie dla warstwy konwergencji. To zdarzenie może być logicznie powiązane ze zdalnym zgłoszeniem usługi lub może być spowodowane przez zdarzenia wewnętrzne MAC. Prymitywy odpowiedzi (.response) przekazywane są z warstwy konwergencji do MAC w celu zapewnienia odpowiedzi na prymityw .indication. Tym samym cztery prymitywy stosowane są w parach - parze .request i .confirm oraz w parze .indication i .response. Pokazano to na Rys. 55, Rys. 56, Rys. 57 i Rys. 58.



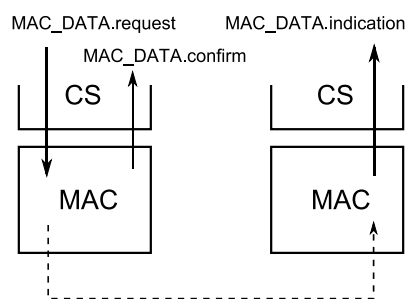
Rys. 55 – Ustanawianie połączenia



Rys. 56 – Niepowodzenie ustanawiania połączenia



Rys. 57 – Zwolnienie połączenia



Rys. 58- Transfer danych

Tabela 33 przedstawia listę dostępnych prymitywów w SAP warstwy MAC:

Tabela 33 – Lista prymitywów MAC

Prymitywy węzła serwisowego	Prymitywy węzła podstawowego
MAC_ESTABLISH.request	MAC_ESTABLISH.request
MAC_ESTABLISH.indication	MAC_ESTABLISH.indication

Prymitywy węzła serwisowego	Prymitywy węzła podstawowego
MAC_ESTABLISH.response	MAC_ESTABLISH.response
MAC_ESTABLISH.confirm	MAC_ESTABLISH.confirm
MAC_RELEASE.request	MAC_RELEASE.request
MAC_RELEASE.indication	MAC_RELEASE.indication
MAC_RELEASE.response	MAC_RELEASE.response
MAC_RELEASE.confirm	MAC_RELEASE.confirm
MAC_JOIN.request	MAC_JOIN.request
MAC_JOIN.Response	MAC_JOIN.response
MAC_JOIN.indication	MAC_JOIN.indication
MAC_JOIN.confirm	MAC_JOIN.confirm
MAC_LEAVE.request	MAC_LEAVE.request
MAC_LEAVE.indication	MAC_LEAVE.indication
MAC_LEAVE.confirm	MAC_LEAVE.confirm
MAC_DATA.request	MAC_REDIRECT.response
MAC_DATA.confirm	MAC_DATA.request
MAC_DATA.indication	MAC_DATA.confirm
	MAC_DATA.indication

1943 4.5.2 Prymitywy sygnalizacji węzła serwisowego i węzła podstawowego

1944 4.5.2.1 Ogólne

1945 Poniższe podpunkty opisują prymitywy, które są dostępne w węźle serwisowym i węźle podstawowym
 1946 MAC-SAP. Są to wyłącznie prymitywy sygnalizujące i stosowane do ustanawiania i zwalniania połączeń
 1947 MAC.

1948 4.5.2.2 MAC_ESTABLISH

1949 4.5.2.2.1 Ogólne

1950 Prymitywy MAC_ESTABLISH są używane do zarządzania procesem ustanawiania połączenia.

1951 4.5.2.2.2 MAC_ESTABLISH.request

1952 Prymityw MAC_ESTABLISH.request jest przekazywany do jednostki warstwy MAC w celu żądania
 1953 ustanowienia połączenia.

1954 Semantyka tego prymitywu przedstawia się następująco:

1955 **MAC_ESTABLISH.request{EUI-48, Type, Data, DataLength, ARQ, CfBytes}**

1956 Parametr *EUI-48* stosowany jest przez węzeł podstawowy do określania adresu węzła, do którego
 1957 adresowane będzie to połączenie. MAC wewnętrznie przeniesie go na adres używany przez warstwę MAC.
 1958 Gdy warstwa konwergencji węzła serwisowego chce połączyć się z węzłem podstawowym, wykorzystuje
 1959 ona identyfikator EUI-48 00:00:00:00:00:00. Jednak, gdy warstwa konwergencji węzła serwisowego chce
 1960 połączyć się z innym węzłem serwisowym w podsieci, wykorzystuje ona identyfikator EUI-48 tego węzła
 1961 serwisowego. To z kolei będzie powodować bezpośrednie nawiązanie połączenia. Jednakże, to czy
 1962 ustanawiane jest normalne czy przekierowywane połączenie, jest oczywiste dla SPA warstwy MAC węzła
 1963 serwisowego. Ponieważ EUI-48 węzła podstawowego jest adresem podsieci, połączenie może zostać
 1964 również zażądane z węzła podstawowego za pomocą adresu podsieci SNA.

1965 Parametr *Type* to identyfikator stosowany do określania typu warstwy konwergencji, która powinna być
 1966 stosowana dla tego połączenia (patrz Załącznik E). Ten parametr ma długość 1 bajta i przesyłany jest w polu
 1967 żądania połączenia CON.TYPE.

1968 Parametr danych *Data* to bufor uniwersalny zamieniany na negocjacje pomiędzy zdalną a lokalną warstwą
 1969 konwergencji. Ten parametr będzie wysyłany w polu żądania połączenia CON.DATA.

1970 Parametr *DataLength* określa długość parametru *Data* w bajtach.

1971 Parametr ARQ wskazuje, czy mechanizm ARQ ma być używany do tego połączenia. Jest to typ logiczny o
 1972 wartości PRAWDA, wskazujący, że zastosowane zostanie Automatyczne żądanie powtórzenia.

1973 Parametr *CfBytes* stosowany jest do wskazania czy połączenie powinno korzystać ze schematu
 1974 bezkolizyjnego czy kolizyjnego dostępu do kanału. Gdy wartość *CfBytes* wynosi zero, należy stosować
 1975 dostęp bezkolizyjny. Gdy wartość *CfBytes* nie wynosi zero, wskazuje ona ile bajtów na ramkę powinno być
 1976 przydzielane do połączenia za pomocą pakietów CFP.

1977 **4.5.2.2.3 MAC_ESTABLISH.indication**

1978 Prymityw MAC_ESTABLISH.indication przekazywany jest z warstwy MAC w celu wskazania, że ustanawianie
 1979 połączenia zostało zainicjowane przez węzeł zdalny.

1980 Semantyka tego prymitywu przedstawia się następująco:

1981 **MAC_ESTABLISH.indication{ConHandle, EUI-48, Type, Data, DataLength, CfBytes}**

1982 *ConHandle* to unikalny identyfikator wymieniany, aby w unikalny sposób zidentyfikować wskazywane
 1983 połączenie. Ma on znaczenie tylko w SAP MAC używanym dla celów odniesienia do tego połączenia
 1984 pomiędzy różnymi prymitywami.

1985 Parametr *EUI-48* wskazuje, które urządzenie w podsieci chce nawiązać połączenie.

1986 Parametr *Type* to identyfikator stosowany do określania typu warstwy konwergencji, która powinna być
 1987 stosowana dla tego połączenia. Ten parametr ma długość 1 bajta i odbierany jest w polu żądania połączenia
 1988 CON.TYPE.

1989 Parametr *Data* to bufor uniwersalny zamieniany na negocjacje pomiędzy zdalną a lokalną warstwą
1990 konwergencji. Ten parametr odbierany jest w polu żądania połączenia CON.DATA.

1991 Parametr *DataLength* określa długość parametru *Data* w bajtach.

1992 Parametr *CfBytes* stosowany jest do wskazania czy połączenie powinno korzystać ze schematu
1993 bezkolizyjnego czy kolizyjnego dostępu do kanału. Gdy *CfBytes* wynosi zero, zastosowany będzie dostęp
1994 bezkolizyjny. Gdy wartość *CfBytes* nie wynosi zero, wskazuje ona ile bajtów na ramkę powinno być
1995 przydzielane do połączenia.

1996 4.5.2.2.4 MAC_ESTABLISH.response

1997 MAC_ESTABLISH.response przesyłany jest do warstwy MAC w celu odpowiedzi na
1998 MAC_ESTABLISH.indication.

1999 Semantyka tego prymitywu przedstawia się następująco:

2000 *MAC_ESTABLISH.response*{*ConHandle*, *Answer*, *Data*, *DataLength*}

2001 Parametr *ConHandle* jest tym samym parametrem, który został odebrany w MAC_ESTABLISH.indication.

2002 Parametr odpowiedzi *Answer* jest używany do zawiadamiania warstwy MAC o działaniu podejmowanym dla
2003 tego ustanawiania połączenia. Parametr ten może przyjąć jedną z wartości podanych w Tabeli 34.

2004 Parametr *Data* to bufor uniwersalny zamieniany na negocjacje pomiędzy zdalną a lokalną warstwą
2005 konwergencji. Ten parametr odbierany jest w polu odpowiedzi połączenia CON.DATA.

2006 Parametr *DataLength* określa długość parametru *Data* w bajtach.

2007 Dane mogą być przekazywane do dzwoniącego, gdy połączenie jest odrzucone, tj. *Answer* (Odpowiedź) ma
2008 wartość 1. Dane te mogą następnie ewentualnie zawierać więcej informacji dotyczących powodu
2009 odrzucenia połączenia.

2010 Tabela 34 – Wartości parametru odpowiedzi *Answer* w prymitywie MAC_ESTABLISH.response

<i>Answer</i> (Odpowiedź)	Opis
<i>Accept</i> = 0	Zatwierdzono ustanawianie połączenia.
<i>Reject</i> = 1	Odrzucono ustanawianie połączenia.

2011 4.5.2.2.5 MAC_ESTABLISH.confirm

2012 Prymityw MAC_ESTABLISH.confirm przekazywany jest z warstwy MAC jako zdana odpowiedź na
2013 MAC_ESTABLISH.request.

2014 Semantyka tego prymitywu przedstawia się następująco:

2015 *MAC_ESTABLISH.confirm*{*ConHandle*, *Result*, *EUI-48*, *Type*, *Data*, *DataLength*}

- 2016 *ConHandle* to unikalny identyfikator w unikalny sposób identyfikujący wskazywane połączenie. Ma on
 2017 znaczenie tylko w SAP MAC używanym dla celów odniesienia do tego połączenia pomiędzy różnymi
 2018 prymitywami. Wartość ta jest prawidłowa jedynie jeśli parametr wyniku *Result* wynosi 0.
- 2019 Parametr wyniku *Result* wskazuje wynik procesu ustanawiania połączenia. Może on przyjąć jedną z wartości
 2020 z Tabela 35.
- 2021 Parametr *EUI-48* wskazuje, które urządzenie w podsieci chce nawiązać połączenie.
- 2022 Parametr *Type* to identyfikator stosowany do określania typu warstwy konwergencji, która powinna być
 2023 stosowana dla tego połączenia. Ten parametr ma długość 1 bajta i odbierany jest w polu żądania połączenia
 2024 CON.TYPE.
- 2025 Parametr *Data* to bufor uniwersalny zamieniany na negocjacje pomiędzy zdalną a lokalną warstwą
 2026 konwergencji. Ten parametr odbierany jest w polu odpowiedzi połączenia CON.DATA.
- 2027 Parametr *DataLength* określa długość parametru *Data* w bajtach.
- 2028 Dane mogą być przekazywane do dzwoniącego, gdy połączenie jest odrzucone, tj. *Result* (Wynik) ma
 2029 wartość 1. Dane te mogą następnie ewentualnie zawierać więcej informacji dotyczących powodu
 2030 odrzucenia połączenia.

Tabela 35 – Wartości parametru wyniku *Result* w prymitywie MAC_ESTABLISH.confirm

Result (Wynik)	Opis
<i>Success</i> = 0	Ustanawianie połączenia zakończyło się powodzeniem.
<i>Reject</i> = 1	Ustanawianie połączenia nie powiodło się, ponieważ zostało odrzucone przez węzeł zdalny.
<i>Timeout</i> = 2	Przekroczono limit czasu ustanawiania połączenia.
<i>No bandwidth</i> = 3	Brak wystarczającej dostępnej przepustowości do zatwierdzenia tego połączenia bezkolizyjnego.
<i>No Such Device</i> = 4	Nie można odnaleźć urządzenia o adresie docelowym.
<i>Redirect failed</i> = 5	Węzeł podstawowy próbował przeprowadzić przeadresowanie, które nie powiodło się.
<i>Not Registered</i> = 6	Węzeł serwisowy nie jest zarejestrowany.
<i>No More LCIDs</i> = 7	Wszystkie dostępne LCID zostały przydzielone.

2032 4.5.2.3 MAC_RELEASE

2033 4.5.2.3.1 Ogólne

2034 Prymitywy MAC_RELEASE są używane do zwalniania połączenia.

2035 4.5.2.3.2 MAC_RELEASE.request

2036 MAC_RELEASE.request to prymityw stosowany do inicjowania procesu zwalniania połączenia.

2037 Semantyka tego prymitywu przedstawia się następująco:

2038 $MAC_RELEASE.request\{ConHandle\}$

2039 Parametr *ConHandle* określa zwalniane połączenie, które ma zostać zwolnione. Ten uchwyt połączenia to
2040 uchwyt uzyskany w trakcie prymitywów MAC_ESTABLISH.

2041 4.5.2.3.3 MAC_RELEASE.indication

2042 MAC_RELEASE.indication to prymityw stosowany do wskazania, że połączenie jest zwalniane. Może ono
2043 zostać zwolnione z powodu działania zdalnego lub z powodu problemu z łącznością.

2044 Semantyka tego prymitywu przedstawia się następująco:

2045 $MAC_RELEASE.indication\{ConHandle, Reason\}$

2046 Parametr *ConHandle* określa zwalniane połączenie. Ten uchwyt połączenia to uchwyt uzyskany w trakcie
2047 prymitywów MAC_ESTABLISH.

2048 Parametr powodu *Reason* może przyjąć jedną z wartości podanych w Tabela 36.

2049 Tabela 36 – Wartości parametru powodu *Reason* w prymitywie MAC_RELEASE.indication

Powód	Opis
Success = 0	Zwolnienie połączenia zostało zainicjowane przez usługę zdalną.
Error = 1	Połączenie zostało zwolnione z powodu problemu z łącznością.

2050 4.5.2.3.4 MAC_RELEASE.response

2051 MAC_RELEASE.response to prymityw stosowany do odpowiadania na proces zwolnienia połączenia.

2052 Semantyka tego prymitywu przedstawia się następująco:

2053 $MAC_RELEASE.response\{ConHandle, Answer\}$

2054 Parametr *ConHandle* określa zwalniane połączenie. Ten uchwyt połączenia to uchwyt uzyskany w trakcie
2055 prymitywów MAC_ESTABLISH.

2056 Parametr odpowiedzi *Answer* może przyjąć jedną z wartości podanych w Tabela 37. Ten parametr może
2057 mieć wartość „Odrzucony = 1”, ponieważ proces uwalniania połączenie nie może zostać odrzucony.

2058 Tabela 37 – Wartości parametru odpowiedzi *Answer* w prymitywie MAC_RELEASE.response

Answer (Odpowiedź)	Opis
Accept = 0	Zatwierdzono zwolnienie połączenia.

2059

2060 Po wysłaniu MAC_RELEASE.response, *ConHandle* nie jest już ważny i nie powinien być używany.

2061 4.5.2.3.5 MAC_RELEASE.confirm

2062 Prymityw MAC_RELEASE.confirm jest stosowany do potwierdzania, że proces zwalniania połączenia został
2063 zakończony.

2064 Semantyka tego prymitywu przedstawia się następująco:

2065 *MAC_RELEASE.confirm*{*ConHandle*, *Result*}

2066 Parametr *ConHandle* określa zwalniane połączenie. Ten uchwyt połączenia to uchwyt uzyskany w trakcie
2067 prymitywów MAC_ESTABLISH.

2068 Parametr wyniku *Result* może przyjąć jedną z wartości podanych w Tabeli 38.

2069 Tabela 38 – Wartości parametru wyniku *Result* w prymitywie MAC_RELEASE.confirm

<i>Result (Wynik)</i>	Opis
<i>Success</i> = 0	Zwolnienie połączenia powiodło się.
<i>Timeout</i> = 2	Przekroczono limit czasu zwolnienia połączenia.
<i>Not Registered</i> = 6	Węzeł serwisowy nie jest już zarejestrowany.

2070

2071 Po odebraniu MAC_RELEASE.confirm, *ConHandle* nie jest już ważny i nie powinien być używany.

2072 4.5.2.4 MAC_JOIN

2073 4.5.2.4.1 Ogólne

2074 Prymitywy MAC_JOIN stosowane są do dołączania do połączenia broadcast lub multicast i umożliwiają
2075 odbiór takich pakietów.

2076 4.5.2.4.2 MAC_JOIN.request

2077 Stosowany jest prymityw MAC_JOIN.request:

- 2078 • Przez wszystkie węzły: aby dołączyć do ruchu broadcast określonej warstwy konwergencji i
2079 rozpocząć odbieranie tych pakietów
- 2080 • Przez węzły serwisowe: aby dołączyć do określonej grupy multicast
- 2081 • Przez węzły podstawowe: aby zaprosić węzeł serwisowy do dołączenia do określonej grupy multicast

2082 W zależności od tego, które urządzenie wysyła żądanie dołączenia, ten punkt SAP może przyjąć dwa różne
2083 warianty. Pierwszy wariant powinien być stosowany w węzłach podstawowych, a drugi w węzłach
2084 serwisowych:

2085 Semantyka tego prymitywu przedstawia się następująco:

2086 *MAC_JOIN.request{Broadcast, ConHandle, EUI-48, Type, Data, DataLength}*

2087 *MAC_JOIN.request{Broadcast, Type, Data, Datalength}*

2088 Parametr *Broadcast* określa czy operacja dołączania przeprowadzana jest dla połączenia typu broadcast lub
2089 dla działania multicast. Powinien on mieć wartość 1 dla operacji broadcast i 0 dla operacji multicast. W
2090 przypadku działania broadcast, EUI-48, Data, DataLength nie są używane.

2091 Parametr *ConHandle* wskazuje uchwyt połączenia używany dla tego dołączenia do grupy multicast. W
2092 przypadku pierwszego żądania dołączenia do nowej grupy multicast, parametr *ConHandle* zostanie
2093 ustawiony na 0. W przypadku kolejnych dodatków EUI do istniejącej grupy multicast, ConHandle będzie
2094 służyć jako indeks odpowiedniej grupy multicast.

2095 Parametr EUI-48 stosowany jest przez węzeł podstawowy do określania adresu węzła, do którego
2096 adresowane będzie to dołączenie. MAC wewnętrznie przeniesie go na adres używany przez warstwę MAC.
2097 Gdy warstwa konwergencji węzła serwisowego zainicjuje żądanie, wykorzystuje ona identyfikator EUI-48
2098 00:00:00:00:00:00.

2099 Parametr *Type* określa typ warstwy konwergencji, która powinna być stosowana do wysyłania/odbierania
2100 pakietów danych. Ten parametr ma długość 1 bajta i przesyłany jest w polu żądania połączenia MUL.TYPE.

2101 Parametr *Data* to bufor uniwersalny zamieniany na negocjacje pomiędzy zdalną a lokalną warstwą
2102 konwergencji. Ten parametr odbierany jest w polu żądania połączenia MUL.DATA. W przypadku, gdy
2103 warstwa konwergencji obsługuje kilka grup multicast, parametr danych *Data* będzie stosowany do
2104 unikalnego identyfikowania grupy.

2105 Parametr *DataLength* określa długość parametru Data w bajtach.

2106 W przypadku, gdy Broadcast = 1, warstwa MAC będzie bezzwłocznie wysłać prymityw MAC_JOIN.confirm,
2107 ponieważ nie musi ona wykonywać żadnych działań „od końca do końca”. Dla działań multicast prymityw
2108 MAC_JOIN.confirm wysyłany jest jedynie po zakończeniu sygnalizowania za pomocą łącza ładowania węzła
2109 serwisowego/węzła podstawowego.

2110 **4.5.2.4.3 MAC_JOIN.confirm**

2111 Prymityw MAC_JOIN.confirm odbierany jest, aby potwierdzić, że działanie MAC_JOIN.request zostało
2112 ukończone.

2113 Semantyka tego prymitywu przedstawia się następująco:

2114 *MAC_JOIN.confirm{ConHandle, Result}*

2115 *ConHandle* to unikalny identyfikator w unikalny sposób identyfikujący wskazywane połączenie. Ma on
2116 znaczenie tylko w SAP MAC używanym dla celów odniesienia do tego połączenia pomiędzy różnymi
2117 prymitywami. Wartość ta jest prawidłowa jedynie jeśli parametr wyniku *Result* wynosi 0. Gdy warstwa MAC
2118 odbiera pakiety na tym połączeniu, przekazane będą one w górę za pomocą prymitywu
2119 MAC_DATA.indication z tym parametrem *ConHandle*.

2120 Parametr wyniku *Result* wskazuje wynik procesu dołączania do grupy multicast. Może on przyjąć jedną z
2121 wartości podanych w Tabeli 39.

2122 Tabela 39 – Wartości parametru wyniku *Result* w prymitywie *MAC_JOIN.confirm*

<i>Result</i> (Wynik)	Opis
<i>Success</i> = 0	Ustanawianie połączenia zakończyło się powodzeniem.
<i>Reject</i> = 1	Ustanawianie połączenia nie powiodło się, ponieważ zostało odrzucone przez węzeł serwisowy/węzeł podstawowy.
<i>Timeout</i> = 2	Przekroczono limit czasu ustanawiania połączenia.

2123 4.5.2.4.4 *MAC_JOIN.indication*

2124 W węźle podstawowym prymityw *MAC_JOIN.indication* przekazywany jest z warstwy MAC w celu
2125 wskazania, że dołączenie do grupy multicast zostało zainicjowane przez węzeł serwisowy. W węźle
2126 serwisowym stosowany jest on do wskazania, że węzeł podstawowy wysłał zaproszenie do dołączenia do
2127 grupy multicast.

2128 W zależności od typu urządzenia, ten prymityw przyjmuje dwa warianty. Pierwszy wariant poniżej powinien
2129 być użyty dla węzłów podstawowych, a drugi dla węzłów serwisowych:

2130 *MAC_JOIN.indication*{*ConHandle*, *EUI-48*, *Type*, *Data*, *DataLength*}

2131 *MAC_JOIN.indication*(*ConHandle*, *Type*, *Data*, *Datalength*)

2132 *ConHandle* to unikalny identyfikator wymieniany w celu unikalnego identyfikowania wskazywanej grupy
2133 multicast. Ma on znaczenie tylko w SAP MAC używanym dla celów odniesienia do tego połączenia pomiędzy
2134 różnymi prymitywami.

2135 Parametr *EUI-48* wskazuje, które urządzenie w podsieci chce nawiązać połączenie.

2136 Parametr *Type* to identyfikator stosowany do określania typu warstwy konwergencji, która powinna być
2137 stosowana dla tego żądania. Ten parametr ma długość 1 bajta i odbierany jest w polu żądania połączenia
2138 MUL.TYPE.

2139 Parametr *Data* to bufor uniwersalny zamieniany na negocjacje pomiędzy zdalną a lokalną warstwą
2140 konwergencji. Ten parametr odbierany jest w polu żądania połączenia MUL.DATA.

2141 Parametr *DataLength* określa długość parametru *Data* w bajtach.

2142 4.5.2.4.5 *MAC_JOIN.response*

2143 *MAC_JOIN.response* przesyłany jest do warstwy MAC w celu odpowiedzi na *MAC_JOIN.indication*. W
2144 zależności od typu urządzenia, ten prymityw może mieć jedną z dwóch form podanych poniżej. Pierwsza
2145 używana jest w węźle serwisowym, a druga w węźle podstawowym.

2146 Semantyka tego prymitywu przedstawia się następująco:

2147 *MAC_JOIN.response{ConHandle, Answer}*

2148 *MAC_JOIN.response (ConHandle, EUI, Answer)*

2149 Parametr *ConHandle* jest tym samym parametrem, który został odebrany w *MAC_JOIN.indication*.

2150 *EUI* to EUI-48 węzła serwisowego, który wnioskował o dołączenie do grupy multicast.

2151 Parametr odpowiedzi *Answer* jest używany do zawiadamiania warstwy MAC o działaniu podejmowanym dla
2152 żądania dołączenia. Parametr ten może przyjąć jedną z wartości podanych poniżej.

2153 Tabela 40 – Wartości parametru odpowiedzi *Answer* w prymitywie *MAC_ESTABLISH.response*

Answer (Odpowiedź)	Opis
Accept = 0	Dołączenie do grupy multicast zostało zatwierdzone.
Reject = 1	Dołączenie do grupy multicast zostało odrzucone.

2154 4.5.2.5 MAC_LEAVE

2155 4.5.2.5.1 Ogólne

2156 Prymitywy *MAC_LEAVE* stosowane są do opuszczania połączenia broadcast lub multicast.

2157 4.5.2.5.2 MAC_LEAVE.request

2158 Prymityw *MAC_LEAVE.request* stosowany jest do opuszczania ruchu multicast lub broadcast. W zależności
2159 od typu urządzenia, ten prymityw może mieć jedną z dwóch form podanych poniżej. Pierwsza używana jest
2160 w węźle serwisowym, a druga w węźle podstawowym.

2161 Semantyka tego prymitywu przedstawia się następująco:

2162 *MAC_LEAVE.request{ConHandle}*

2163 *MAC_LEAVE.request{ConHandle, EUI}*

2164 Parametr *ConHandle* określa zwalniane połączenie, które ma zostać opuszczone. Ten uchwyt połączenia to
2165 uchwyt uzyskany w trakcie prymitywów *MAC_JOIN*.

2166 *EUI* to EUI-48 węzła serwisowego, który ma zostać usunięty z grupy multicast.

2167 4.5.2.5.3 MAC_LEAVE.confirm

2168 Prymityw *MAC_LEAVE.confirm* odbierany jest, aby potwierdzić, że działanie *MAC_LEAVE.request* zostało
2169 ukończone.

2170 Semantyka tego prymitywu przedstawia się następująco:

2171 *MAC_LEAVE.confirm{ConHandle, Result}*

2172 Parametr *ConHandle* określa zwalniane połączenie. Ten uchwyt połączenia to uchwyt uzyskany w trakcie
2173 prymitywów MAC_JOIN.

2174 Parametr wyniku *Result* może przyjąć jedną z wartości podanych w Tabela 41.

2175 Tabela 41 – Wartości parametru wyniku *Result* w prymitywie MAC_LEAVE.confirm

Result (Wynik)	Opis
<i>Success</i> = 0	Opuszczenie połączenia powiodło się.
<i>Timeout</i> = 2	Przekroczono limit czasu opuszczania połączenia.

2176

2177 Po odebraniu MAC_LEAVE.confirm, ConHandle nie jest już ważny i nie powinien być używany.

2178 4.5.2.5.4 MAC_LEAVE.indication

2179 Prymityw MAC_LEAVE.indication stosowany jest do opuszczania ruchu multicast lub broadcast. W
2180 zależności od typu urządzenia, ten prymityw może mieć jedną z dwóch form podanych poniżej. Pierwsza
2181 używana jest w węźle serwisowym, a druga w węźle podstawowym.

2182 Semantyka tego prymitywu przedstawia się następująco:

2183 *MAC_LEAVE.indication{ConHandle}*

2184 *MAC_LEAVE.indication{ConHandle, EUI}*

2185 Parametr ConHandle jest tym samym parametrem, który został odebrany w MAC_JOIN.confirm lub
2186 MAC_JOIN.indication. Ten uchwyt połączenia to uchwyt uzyskany w trakcie prymitywów MAC_JOIN.

2187 EUI to EUI-48 węzła serwisowego, który ma zostać usunięty z grupy multicast.

2188 4.5.3 Prymitywy sygnalizacji węzła podstawowego

2189 4.5.3.1 Ogólne

2190 Rozdział ten opisuje prymitywy MAC-SAP, które dostępne są tylko w węźle podstawowym.

2191 4.5.3.2 MAC_REDIRECT.response

2192 Prymityw MAC_REDIRECT.response stosowany jest do odpowiadania na MAC_ESTABLISH.indication i
2193 przekierowuje połączenie z węzła podstawowego do innego węzła serwisowego w podsieci.

2194 Semantyka tego prymitywu przedstawia się następująco:

2195 *MAC_REDIRECT.reponse{ConHandle, EUI-48, Data, DataLength}*

2196 ConHandle to parametr przekazywany w prymitywie MAC_ESTABLISH.indication, na który on odpowiada.

2197 *EUI-48* wskazuje węzeł serwisowy, do którego przesłane powinno zostać to ustanowienie sieci. Węzeł
2198 podstawowy powinien przeprowadzić konfigurację połączenia bezpośredniego pomiędzy źródłem
2199 ustanawiania połączenia a węzłem serwisowym wskazanym przez *EUI-48*.

2200 Parametr *Data* to bufor uniwersalny zamieniany na negocjacje pomiędzy zdalną a warstwą konwergencji
2201 węzła podstawowego. Ten parametr odbierany jest w polu żądania połączenia *CON.DATA*.

2202 Parametr *DataLength* określa długość parametru *Data* w bajtach.

2203 Po zastosowaniu tego prymitywu parametr *ConHandle* już nie obowiązuje.

2204 **4.5.4 Prymitywy danych węzła podstawowego i węzła serwisowego**

2205 **4.5.4.1 Ogólne**

2206 Poniższe podpunkty opisują sposób przekazywania danych z węzła serwisowego lub węzła podstawowego
2207 pomiędzy warstwą konwergencji a warstwą MAC.

2208 **4.5.4.2 MAC_DATA.request**

2209 Prymityw *MAC_DATA.request* jest stosowany do inicjowania procesu transmisji danych w połączeniu.

2210 Semantyka tego prymitywu przedstawia się następująco:

2211 *MAC_DATA.request{ConHandle, Data, DataLength, Priority}*

2212 Parametr *ConHandle* określa połączenie, które ma zostać zastosowane do transmisji danych. Ten uchwyt
2213 połączenia to uchwyt uzyskany w trakcie prymitywów ustanawiania połączenia.

2214 Parametr danych *Data* jest buforem oktetów które zawierają dane warstwy konwergencji przesyłane przez
2215 to połączenie.

2216 Parametr *DataLength* określa długość parametru *Data* w oktetach.

2217 *Priorytet* wskazuje priorytet danych, które mają zostać wysłane podczas korzystania ze schematu dostępu
2218 CSMA, tj. parametr jest poprawny wyłącznie, jeśli połączenie zostało ustanowione z *CfBytes = 0*.

2219 **4.5.4.3 MAC_DATA.confirm**

2220 Prymityw *MAC_DATA.confirm* jest stosowany do potwierdzania, że proces transmisji danych został
2221 zakończony.

2222 Semantyka tego prymitywu przedstawia się następująco:

2223 *MAC_DATA.confirm{ConHandle, Data, Result}*

2224 Parametr *ConHandle* określa połączenie zastosowane do transmisji danych. Ten uchwyt połączenia to
2225 uchwyt uzyskany w trakcie prymitywów ustanawiania połączenia.

2226 Parametr danych *Data* jest buforem oktetów które zawierają dane warstwy konwergencji, które zostały
2227 przesyłane przez to połączenie.

2228 Parametr wyniku *Result* wskazuje wynik transmisji. Może on przyjąć jedną z wartości podanych w Tabeli
2229 42.

2230 Tabela 42 – Wartości parametru wyniku *Result* w prymitywie *MAC_DATA.confirm*

<i>Result</i> (Wynik)	Opis
<i>Success</i> = 0	Wysyłanie powiodło się.
<i>Timeout</i> = 2	Czas procesu wysyłania upłynął.

2231 4.5.4.4 *MAC_DATA.indication*

2232 Prymityw *MAC_DATA.indication* powiadamia o odebraniu danych przez połączenie z warstwą
2233 konwergencji.

2234 Semantyka tego prymitywu przedstawia się następująco:

2235 *MAC_DATA.indication*{*ConHandle*, *Data*, *DataLength*}

2236 Parametr *ConHandle* określa połączenie, w którym otrzymane zostały dane. Ten uchwyt połączenia to
2237 uchwyt uzyskany w trakcie prymitywów ustanawiania połączenia.

2238 Parametr danych *Data* jest buforem oktetów które zawierają dane warstwy konwergencji odebrane przez
2239 to połączenie.

2240 Parametr *DataLength* określa długość parametru *Data* w oktetach.

2241 4.5.5 SAP jednostki zarządzającej warstwą MAC

2242 4.5.5.1 Ogólne

2243 Następujące prymitywy są opcjonalne.

2244 Ich celem jest umożliwienie zewnętrznej jednostce zarządzającej kontrolowanie rejestracji i promocji węzła
2245 serwisowego, degradacji i wyrejestrowywania węzła serwisowego. Warstwa MAC normalnie wykonywałaby
2246 to automatycznie, jednakże w niektórych sytuacjach korzystne było by przeprowadzanie tych procesów
2247 przez jednostki zewnętrzne. Istnieją również wskazania, aby podmiot zewnętrzny mógł monitorować status
2248 MAC.

2249 4.5.5.2 *MLME_REGISTER*

2250 4.5.5.2.1 Ogólne

2251 Prymitywy *MLME_REGISTER* są stosowane do przeprowadzania rejestracji i wskazywania, kiedy
2252 przeprowadzona została rejestracja.

2253 4.5.5.2.2 *MLME_REGISTER.request*

2254 Prymityw *MLME_REGISTER.request* stosowany jest do włączania procesu rejestrowania do podsieci za
2255 pośrednictwem określonego węzła przełączającego. Ten prymityw może być stosowany do wymuszania

2256 wyboru określonego węzła przełączającego, który niekoniecznie musi zostać wybrany, jeśli wybór będzie
2257 automatyczny. Funkcja MLME węzła podstawowego nie eksportuje tego prymitywu.

2258 Semantyka tego prymitywu mogłaby wyglądać następująco:

2259 *MLME_REGISTER.request{ }*

2260 Wywołanie tego prymitywu bez parametrów po prostu wywołuje proces rejestracji w MAC i pozostawia
2261 wybór węzła podsieci i węzłów przełączających w decyzji algorytmów MAC. Korzystanie z tego prymitywu
2262 umożliwia MAC przeprowadzanie w pełni automatycznej rejestracji, jeśli taki tryb jest realizowany w MAC.

2263 *MLME_REGISTER.request{SNA}*

2264 Parametr *SNA* określa podsieć, dla której przeprowadzana powinna być rejestracja. Wywoływanie
2265 prymitywu w tym formacie nakazuje warstwie MAC zarejestrowanie się tylko w określonej podsieci.

2266 *MLME_REGISTER.request{SID}*

2267 Parametr *SID* to *SID* (Identyfikator przełączenia) Węzła przełączającego, przez który przeprowadzana musi
2268 zostać rejestracja. Wywoływanie prymitywu w tym formacie nakazuje warstwie MAC zarejestrowanie się
2269 tylko w określonym węźle przełączającym.

2270 **4.5.5.2.3 MLME_REGISTER.confirm**

2271 Prymityw *MLME_REGISTER.confirm* służy do potwierdzenia statusu zakończenia procesu rejestracyjnego,
2272 który został zainicjowany przez wcześniejsze wywołanie odpowiedniego prymitywu żądania. Funkcja MLME
2273 węzła podstawowego nie eksportuje tego prymitywu.

2274 Semantyka tego prymitywu przedstawia się następująco:

2275 *MLME_REGISTER.confirm{Result, SNA, SID}*

2276 Parametr *Result* wskazuje wynik Rejestracji. Może on przyjąć jedną z wartości podanych w Tabeli 43.

2277 **Tabela 43 – Wartości parametru wyniku *Result* w prymitywie *MLME_REGISTER.confirm***

<i>Result</i> (Wynik)	Opis
<i>Done</i> = 0	Rejestracja do określonego adresu podsieci poprzez określone przełączenie zakończyła się powodzeniem.
<i>Timeout</i> = 2	Upłynął limit czasu żądania rejestracji.
<i>Rejected</i> =1	Żądanie rejestracji jest odrzucane przez węzeł podstawowy określonego <i>SNA</i> .
<i>NoSNA</i> =8	Określony adres podsieci nie mieści się w zakresie.
<i>NoSwitch</i> =9	Węzeł przełączający z określonym <i>EUI-48</i> nie mieści się w zakresie.

2278 Parametr *SNA* określa podsieć, dla której przeprowadzana jest rejestracja. Parametr jest prawidłowy
2279 jedynie jeśli *Result*=0.

2280 Parametr *SID* to *SID* (Identyfikator przełączenia) Węzła przełączającego, przez który przeprowadzana jest
2281 rejestracja. Parametr jest prawidłowy jedynie jeśli *Result=0*.

2282 4.5.5.2.4 MLME_REGISTER.indication

2283 Prymityw *MLME_REGISTER.indication* stosowany jest do wskazywania zmiany statusu w warstwie MAC.
2284 Węzeł serwisowy jest teraz zarejestrowany w podsieci.

2285 Semantyka tego prymitywu przedstawia się następująco:

2286 *MLME_REGISTER.indication{SNA, SID}*

2287 Parametr *SNA* określa podsieć, dla której przeprowadzana jest rejestracja.

2288 Parametr *SID* to *SID* (Identyfikator przełączenia) Węzła przełączającego, przez który przeprowadzana jest
2289 rejestracja.

2290 4.5.5.3 MLME_UNREGISTER

2291 4.5.5.3.1 Ogólne

2292 Prymitywy *MLME_UNREGISTER* są stosowane do przeprowadzania wyrejestrowywania i wskazywania,
2293 kiedy przeprowadzony został proces wyrejestrowania.

2294 4.5.5.3.2 MLME_UNREGISTER.request

2295 Prymityw *MLME_UNREGISTER.request* stosowany jest do włączania procesu wyrejestrowywania. Ten
2296 prymityw może być stosowany przez jednostki zarządzające, jeśli wymagają one od węzła wyrejestrowania
2297 z jakiegoś powodu (np. rejestracji przez kolejny węzeł przełączający lub do innej podsieci). Funkcja *MLME*
2298 węzła podstawowego nie eksportuje tego prymitywu.

2299 Semantyka tego prymitywu przedstawia się następująco:

2300 *MLME_UNREGISTER.request{}*

2301 4.5.5.3.3 MLME_UNREGISTER.confirm

2302 Prymityw *MLME_UNREGISTER.confirm* służy do potwierdzenia statusu zakończenia procesu
2303 wyrejestrowania, który został zainicjowany przez wcześniejsze wywołanie odpowiedniego prymitywu
2304 żądania. Funkcja *MLME* węzła podstawowego nie eksportuje tego prymitywu.

2305 Semantyka tego prymitywu przedstawia się następująco:

2306 *MLME_UNREGISTER.confirm{Result}*

2307 Parametr *Result* wskazuje wynik Rejestracji. Może on przyjąć jedną z wartości podanych w Tabeli 44.

2308 Tabela 44 – Wartości parametru wyniku *Result* w prymitywie *MLME_UNREGISTER.confirm*

<i>Result (Wynik)</i>	Opis
<i>Done = 0</i>	Proces wyrejestrowania zakończył się powodzeniem.

Result (Wynik)	Opis
<i>Timeout = 2</i>	Czas procesu wyrejestrowywania upłynął.
<i>Redundant=10</i>	Węzeł znajduje się już w stanie <i>Rozłączony</i> i nie wymaga wyrejestrowywania.

2309

2310 Po wygenerowaniu MLME_UNREGISTER.confirm, warstwa MAC nie powinna przeprowadzać żadnych
 2311 działań automatycznych, które mogą ponownie wywołać proces rejestracji. W takich przypadkach od
 2312 jednostki zarządzającej zależy ponowne uruchomienie funkcjonalności MAC z odpowiednimi prymitywami
 2313 MLME_REGISTER.

2314 **4.5.5.3.4 MLME_UNREGISTER.indication**

2315 Prymityw MLME_UNREGISTER.indication stosowany jest do wskazywania zmiany statusu w warstwie MAC.
 2316 Węzeł serwisowy nie jest już zarejestrowany w podsięci.

2317 Semantyka tego prymitywu przedstawia się następująco:

2318 *MLME_UNREGISTER.indication{}*

2319 **4.5.5.4 MLME_PROMOTE**

2320 **4.5.5.4.1 Ogólne**

2321 Prymitywy MLME_PROMOTE są stosowane do przeprowadzania promocji i wskazywania, kiedy
 2322 przeprowadzony został proces promocji.

2323 **4.5.5.4.2 MLME_PROMOTE.request**

2324 Prymityw MLME_PROMOTE.request jest stosowany do uruchamiania procesu promocji w węźle
 2325 serwisowym, który znajduje się w stanie funkcjonalnym *Terminal*. Ten prymityw może być stosowany przez
 2326 jednostki zarządzające do wymuszania promocji w przypadkach, gdy domyślna funkcjonalność węzła nie
 2327 uruchamia procesu automatycznie. Wdrożenia mogą stosować takie wyzwalane promocje do okresowej
 2328 optymalizacji topologii podsięci.

2329 Semantyka tego prymitywu przedstawia się następująco:

2330 *MLME_PROMOTE.request{}*

2331 Wartość PRO.PNA w komunikacie promocji wysyłana do węzła podstawowego jest nieokreślona i właściwa
 2332 dla implementacji.

2333 **4.5.5.4.3 MLME_PROMOTE.confirm**

2334 Prymityw MLME_PROMOTE.confirm służy do potwierdzenia statusu zakończenia procesu promocji, który
 2335 został zainicjowany przez wcześniejsze wywołanie odpowiedniego prymitywu żądania.

2336 Semantyka tego prymitywu przedstawia się następująco:

2337 *MLME_PROMOTE.confirm{Result}*

2338 Parametr *Result* wskazuje wynik Rejestracji. Może on przyjąć jedną z wartości podanych w Tabeli 45.

2339 **Tabela 45 – Wartości parametru wyniku *Result* w prymitywie *MLME_PROMOTE.confirm***

<i>Result (Wynik)</i>	<i>Opis</i>
<i>Done = 0</i>	Węzeł został z powodzeniem promowany do funkcji Przełączania.
<i>Timeout = 1</i>	Czas procesu promocji upłynął.
<i>Rejected=2</i>	Węzeł podstawowy odrzucił żądanie promocji.
<i>Redundant=10</i>	Urządzenie to już działa jako węzeł przełączający.

2340 **4.5.5.4.4 MLME_PROMOTE.indication**

2341 Prymityw *MLME_PROMOTE.indication* stosowany jest do wskazywania zmiany statusu w warstwie MAC.
 2342 Węzeł serwisowy działa teraz jako Przełączenie.

2343 Semantyka tego prymitywu przedstawia się następująco:

2344 *MLME_PROMOTE.indication{}*

2345 **4.5.5.5 MLME_DEMOTE**

2346 **4.5.5.5.1 Ogólne**

2347 Prymitywy *MLME_DEMOTE* są stosowane do przeprowadzania degradacji i wskazywania, kiedy
 2348 przeprowadzony został proces degradacji.

2349 **4.5.5.5.2 MLME_DEMOTE.request**

2350 Prymityw *MLME_DEMOTE.request* jest stosowany do uruchamiania procesu degradacji w węźle
 2351 serwisowym, który znajduje się w stanie funkcjonalnym *Przełączenie*. Ten prymityw może być stosowany
 2352 przez jednostki zarządzające do wymuszania degradacji w przypadkach, gdy domyślna funkcjonalność węzła
 2353 nie uruchamia procesu automatycznie.

2354 Semantyka tego prymitywu przedstawia się następująco:

2355 *MLME_DEMOTE.request{}*

2356 **4.5.5.5.3 MLME_DEMOTE.confirm**

2357 Prymityw *MLME_DEMOTE.confirm* służy do potwierdzenia statusu zakończenia procesu degradacji, który
 2358 został zainicjowany przez wcześniejsze wywołanie odpowiedniego prymitywu żądania.

2359 Semantyka tego prymitywu przedstawia się następująco:

2360 *MLME_DEMOTE.confirm{Result}*

2361 Parametr wyniku *Result* wskazuje wynik degradacji. Może on przyjąć jedną z wartości podanych w Tabeli
 2362 46.

2363 **Tabela 46 – Wartości parametru wyniku *Result* w prymitywie *MLME_DEMOTE.confirm***

Result (Wynik)	Opis
<i>Done = 0</i>	Węzeł został skutecznie zdegradowany do funkcji Terminala.
<i>Timeout = 1</i>	Czas procesu degradacji upłynął.
<i>Redundant=10</i>	Urządzenie to już działa jako węzeł Terminala.

2364

2365 Gdy degradacja została uruchomiona za pomocą MLME_DEMOTE.request, Terminal pozostanie
2366 zdegradowany.

2367 **4.5.5.5.4 MLME_DEMOTE.indication**

2368 Prymityw MLME_DEMOTE.indication stosowany jest do wskazywania zmiany statusu w warstwie MAC.
2369 Węzeł serwisowy działa teraz jako Terminal.

2370 Semantyka tego prymitywu przedstawia się następująco:

2371 *MLME_DEMOTE.indication{}*

2372 **4.5.5.6 MLME_RESET**

2373 **4.5.5.6.1 Ogólne**

2374 Prymitywy MLME_RESET stosowane są do resetowania MAC do znanego dobrego statusu.

2375 **4.5.5.6.2 MLME_RESET.request**

2376 Prymityw MLME_RESET.request prowadzi do resetowania wszystkich buforów wysyłających i odbierających
2377 i wyzerowanie wszystkich zmiennych stanów. W wyniku wywołania tego prymitywu węzeł serwisowy
2378 przejdzie z bieżącego stanu funkcjonalnego do stanu funkcjonalnego *Rozłączony*.

2379 Semantyka tego prymitywu przedstawia się następująco:

2380 *MLME_RESET.request{}*

2381 **4.5.5.6.3 MLME_RESET.confirm**

2382 Prymityw MLME_RESET.confirm służy do potwierdzenia statusu zakończenia procesu resetowania, który
2383 został zainicjowany przez wcześniejsze wywołanie odpowiedniego prymitywu żądania. Po udanym
2384 zakończeniu procesu resetowania jednostka MAC powinna ponownie uruchomić wszystkie funkcje,
2385 począwszy od wyszukiwania podsieci (4.3.1).

2386 Semantyka tego prymitywu przedstawia się następująco:

2387 *MLME_RESET.confirm{Result}*

2388 Parametr wyniku *Result* wskazuje wynik resetowania. Może on przyjąć jedną z wartości podanych poniżej.

2389 **Tabela 47 – Wartości parametru wyniku *Result* w prymitywie MLME_RESET.confirm**

Result (Wynik)	Opis
<i>Done = 0</i>	Resetowanie MAC zakończyło się powodzeniem.
<i>Failed =1</i>	Błąd resetowania MAC z przyczyn wdrożeń wewnętrznych.

2390 4.5.5.7 MLME_GET

2391 4.5.5.7.1 Ogólne

2392 Prymitywy MLME_GET stosowane są do odzyskiwania pojedynczych wartości, takich jak statystyki, z
2393 warstwy MAC.

2394 4.5.5.7.2 MLME_GET.request

2395 Prymityw MLME_GET.request wysyła zapytania dotyczące danego atrybutu PIB.

2396 Semantyka tego prymitywu przedstawia się następująco:

2397 *MLME_GET.request{PIBAttribute}*

2398 Parametr *PIBAttribute* określa konkretne atrybuty wymienione w tabeli w pozycji *Id* , które wyliczają
2399 atrybuty PIB (Punkt 6.2.3).

2400 4.5.5.7.3 MLME_GET.confirm

2401 Prymityw MLME_GET.confirm generowany jest w odpowiedzi na prymityw MLME_GET.request.

2402 Semantyka tego prymitywu przedstawia się następująco:

2403 *MLME_GET.confirm{status, PIBAttribute, PIBAttributeValue}*

2404 Parametr *status* podaje wynik żądanych informacji i może przyjąć jedną z wartości podanych w Tabela 48.

2405 Tabela 48 – Wartości parametru statusu w prymitywie MLME_GET.confirm

Result (Wynik)	Opis
<i>Done = 0</i>	Wczytanie parametru powiodło się.
<i>Failed =1</i>	Błąd wczytywania parametru z przyczyn wdrożeń wewnętrznych.
<i>BadAttr=11</i>	Określony atrybut <i>PIBAttribute</i> nie jest obsługiwany.

2406

2407 Parametr *PIBAttribute* określa konkretne atrybuty wymienione w tabeli w pozycji *Id* , które wyliczają
2408 atrybuty PIB (Punkt 6.2.3.5).

2409 Parametr wartości *PIBAtributeValue* określa wartość związaną z danym atrybutem *PIBAtribute*

2410 4.5.5.8 MLME_LIST_GET

2411 4.5.5.8.1 Ogólne

2412 Prymitywy MLME_LIST_GET stosowane są do odzyskiwania listy wartości z MAC.

2413 4.5.5.8.2 MLME_LIST_GET.request

2414 Zapytania MLME_LIST_GET.request dla listy wartości odnoszącej się do określonej klasy. Ta specjalna klasa
2415 atrybutów PIB podana została w Tabeli 96.

2416 Semantyka tego prymitywu przedstawia się następująco:

2417 *MLME_LIST_GET.request{PIBListAttribute}*

2418 Parametr *PIBListAttribute* identyfikuje określoną listę wymaganą przez jednostkę zarządzającą. Możliwe
2419 wartości *PIBListAttribute* podano w 6.2.3.5.

2420 4.5.5.8.3 MLME_LIST_GET.confirm

2421 Prymityw MLME_LIST_GET.confirm generowany jest w odpowiedzi na odpowiedni prymityw
2422 MLME_LIST_GET.request.

2423 Semantyka tego prymitywu przedstawia się następująco:

2424 *MLME_LIST_GET.confirm{status, PIBListAttribute, PIBListAttributeValue}*

2425 Parametr *status* podaje wynik żądanych informacji i może przyjąć jedną z wartości podanych w Tabeli 49.

2426 Tabela 49 – Wartości parametru statusu w prymitywie MLME_LIST_GET.confirm

Result (Wynik)	Opis
<i>Done = 0</i>	Wczytanie parametru powiodło się.
<i>Failed =1</i>	Błąd wczytywania parametru z przyczyn wdrożeń wewnętrznych.
<i>BadAttr=11</i>	Określony atrybut <i>PIBListAttribute</i> nie jest obsługiwany.

2427

2428 Parametr *PIBListAttribute* identyfikuje określoną listę zgodnie z polem ID w Tabeli 96.

2429 Parametr wartości *PIBAttributeValue* zawiera rzeczywistą listę związaną z danym atrybutem *PIBAttribute*

2430 4.5.5.9 MLME_SET

2431 4.5.5.9.1 Ogólne

2432 Prymitywy MLME_SET stosowane są do ustawiania wartości konfiguracyjnych w MAC.

2433 4.5.5.9.2 MLME_SET.request

2434 Prymityw MLME_SET.request wymaga informacji na temat danego atrybutu PIB.

2435 Semantyka tego prymitywu przedstawia się następująco:

2436 *MLME_SET.request{PIBAttribute, PIBAttributeValue}*

2437 Parametr *PIBAttribute* określa konkretne atrybuty wymienione w tabeli w pozycji *Id* , które wyliczają
2438 atrybuty PIB (Punkt 6.2.3).

2439 Parametr wartości *PIBAttributeValue* określa wartość związaną z danym atrybutem *PIBAttribute*.

2440 4.5.5.9.3 MLME_SET.confirm

2441 Prymityw MLME_SET.confirm generowany jest w odpowiedzi na prymityw MLME_SET.request.

2442 Semantyka tego prymitywu przedstawia się następująco:

2443 *MLME_SET.confirm{result}*

2444 Parametr wyniku *result* podaje wynik żądanych informacji i może przyjąć jedną z wartości podanych w
2445 Tabela 50.

2446 Tabela 50 – Wartości parametru wyniku *Result* w prymitywie MLME_SET.confirm

Result (Wynik)	Opis
<i>Done = 0</i>	Podana wartość z powodzeniem ustawiona dla określonego atrybutu.
<i>Failed =1</i>	Nie można ustawić danej wartości dla określonego atrybutu.
<i>BadAttr=11</i>	Określony atrybut <i>PIBAttribute</i> nie jest obsługiwany.
<i>OutOfRange=12</i>	Określony atrybut <i>PIBAttributeValue</i> jest poza dopuszczalnym zakresem.
<i>ReadOnly=13</i>	Określony atrybut <i>PIBAttributeValue</i> jest tylko do odczytu.

2447

2448 Parametr *PIBAttribute* określa konkretne atrybuty wymienione w tabeli w pozycji *Id* , które wyliczają
2449 atrybuty PIB (Punkt 6.2.3).

2450 Parametr wartości *PIBAttributeValue* określa wartość związaną z danym atrybutem *PIBAttribute*

2451 4.6 Procedury MAC

2452 4.6.1 Rejestracja

2453 Po początkowym uruchomieniu węzła serwisowego następuje proces rejestracji (4.3.1). Węzeł serwisowy w
2454 stanie funkcjonalnym *Rozłączony* prześle pakiet kontrolny REG do węzła podstawowego w celu ujęcia w
2455 podsięci. Ponieważ LNID lub SID jest przydzielony na tym etapie do węzła serwisowego, pole PKT.LNID
2456 powinno zostać ustawione na same 1-nki, a pole PKT.SID powinno zawierać SID węzła przełączającego,
2457 przez który szuka on dołączenia do podsięci.

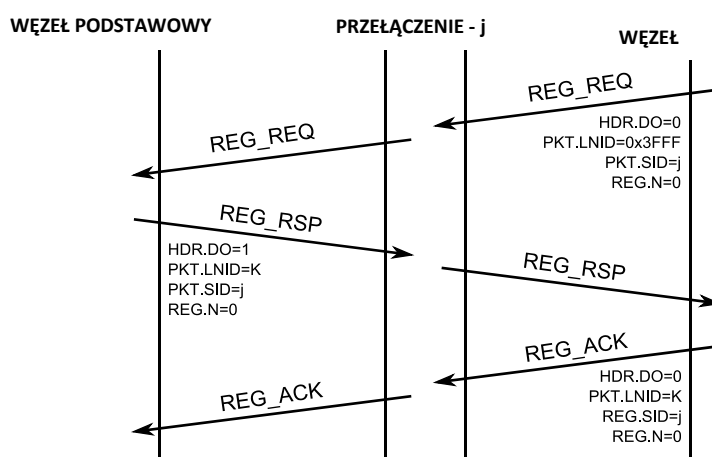
Węzły podstawowe mogą korzystać z żądania rejestracji jako mechanizmu uwierzytelniającego. Jednakże ta specyfikacja nie zaleca, ani nie zakazuje żadnego określonego mechanizmu uwierzytelniania i zostawia ten wybór konkretnym wdrożeniom.

W przypadku wszystkich skutecznie zaakceptowanych żądań rejestracji węzeł podstawowy przydzieli LNID, który jest unikalny w domenie węzła przełączającego przez który realizowane jest przełączanie. Identyfikator LNID powinien być wskazany w polu odpowiedzi PKT.LNID (REG_RSP). Przypisany LNID w połączeniu z SID węzła przełączającego, przez który zarejestrowany jest węzeł serwisowy utworzy NID węzła rejestrującego.

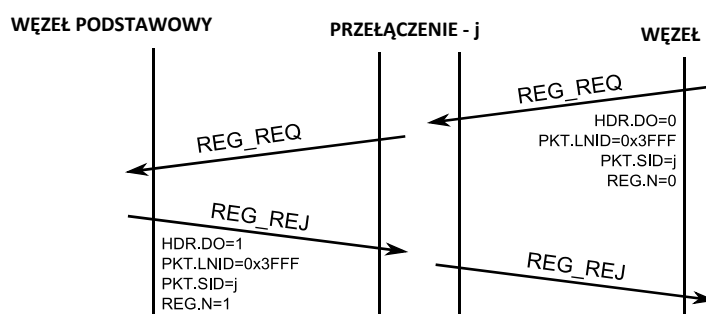
Rejestracja jest procesem trójstronnym. REG_RSP powinien zostać zatwierdzony przez odbierający węzeł serwisowy za pomocą komunikatu REG_ACK.

Rys. 59 reprezentuje skuteczny proces rejestracji Rys. 60 pokazuje żądanie rejestracji, która jest odrzucona przez węzeł podstawowy. W Tabeli 15 podano szczegółowe pola, które odróżniają od siebie komunikaty rejestracji.

Pakiet kontrolny REG, wraz ze wszystkimi wariantami użycia, jest przesyłany niezaszyfrowany, ale określone pola (REG.SNK i REG.AUK) są zaszyfrowane zależnymi od kontekstu kluczami, jak wyjaśniono w punkcie 4.4.5.3. Szyfrowanie REG.AUK w REG_RESP, deszyfrowanie po stronie odbiorczej i kolejne retransmisje szyfrowane przy użyciu innego klucza szyfrowania uwierzytelniają, że REG_ACK pochodzi z zamierzonego punktu docelowego.



Rys. 59 – Zatwierdzony proces rejestracji



Rys. 60 – Odrzucony proces rejestracji

Podczas przydzielania LNID, węzeł podstawowy nie powinien ponownie używać LNID, zwolnionego przez proces wyrejestrowywania aż do $(macMaxCtlReTx + 1) * macCtlReTxTimer$ sekund, aby zapewnić, że

wszystkie pakiety retransmisji opuściły podsieć. Podobnie węzeł podstawowy nie powinien ponownie używać LNID uwolnionego przez proces Utrzymywania aktywności do czasu upływu $T_{\text{keep_alive}}$ sekund za pomocą ostatniej znanej zatwierdzonej wartości $T_{\text{keep_alive}}$, lub jeśli większa, ostatniej niezatwierdzonej wartości $T_{\text{keep_alive}}$, dla węzła serwisowego za pomocą LNID.

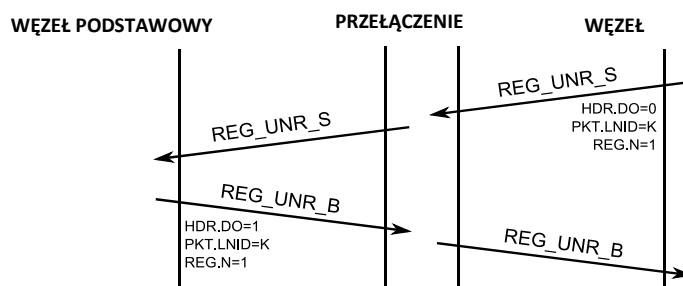
W czasie uruchamiania sieci, gdy cała sieć jest zasilana jednorazowo, nastąpi konflikt dostępu do medium. Zalecane, ale nieobowiązkowe, aby losowość dodawana była do pierwszej transmisji REQ_REQ i wszystkich kolejnych retransmisji. Losowe opóźnienie o maksymalnym czasie trwania równym 10% *macCtReTxTimer* może być narzucone przed pierwszym komunikatem REG_REQ, a podobne losowe opóźnienie do 10% *macCtReTxTimer* może zostać dodane do każdej retransmisji.

4.6.2 Proces wyrejestrowywania

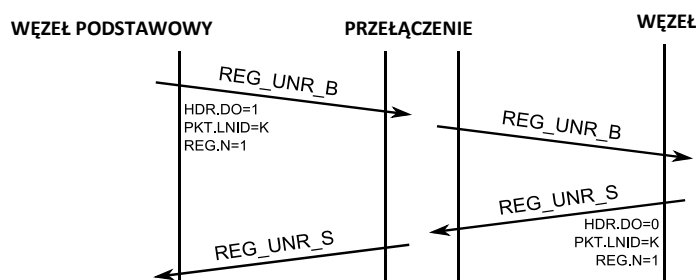
W dowolnym momencie w czasie albo węzeł podstawowy, albo węzeł serwisowy może zdecydować o zamknięciu istniejącej rejestracji. Ta wersja specyfikacji nie zawiera informacji na temat odrzucania żądania wyrejestrowywania. Węzeł serwisowy lub węzeł podstawowy, który odbiera żądanie wyrejestrowywania powinien zatwierdzić jego odebranie i podjąć odpowiednie działania.

Po udanym wyrejestrowaniu węzeł serwisowy powinien przejść za aktualnego stanu funkcjonalnego do stanu funkcjonalnego *Rozłączony*, a węzeł podstawowy może ponownie skorzystać z dowolnych zasobów, które były zarezerwowane dla wyrejestrowanego węzła.

Rys. 61 pokazuje skuteczny proces wyrejestrowania inicjowany z węzła serwisowego, a Rys. 62 pokazuje proces wyrejestrowania inicjowany z węzła podstawowego. W Tabeli 15 podano szczegółowe pola, które identyfikują żądania wyrejestrowania w pakietach kontrolnych REG.



Rys. 61 – Proces wyrejestrowania inicjowany przez węzeł terminala



Rys. 62 – Proces wyrejestrowania inicjowany przez węzeł podstawowy

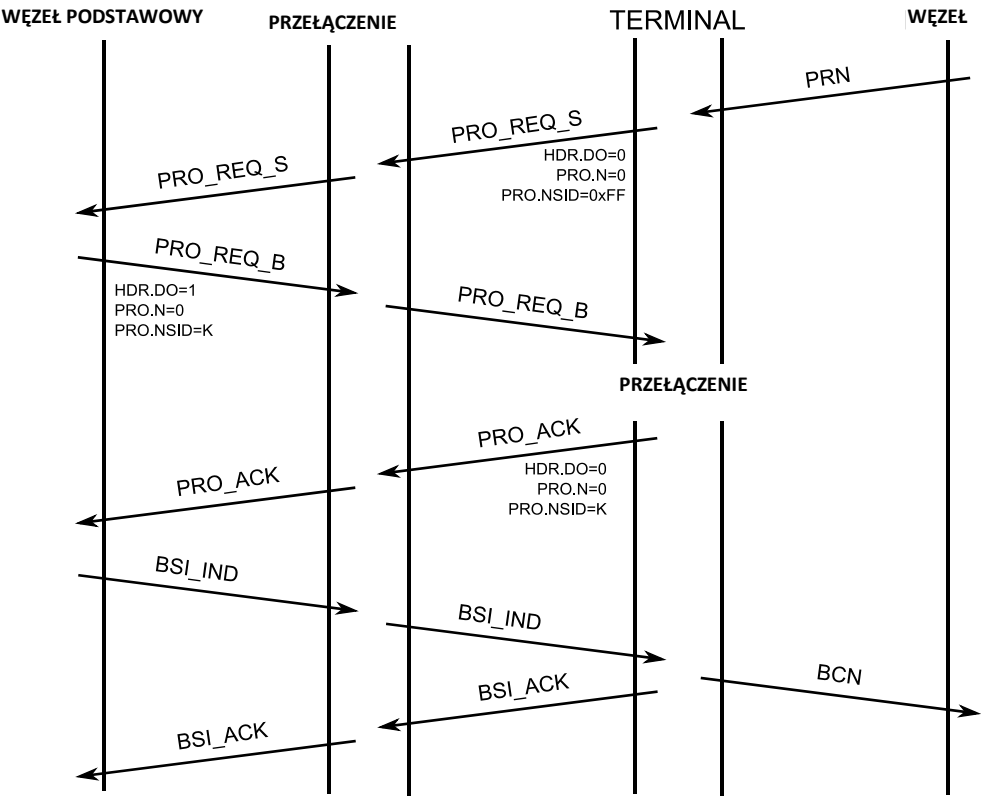
2507 4.6.3 Proces promocji

2508 Węzeł, który nie może osiągnąć istniejącego przełączenia może wysłać ramki wymagane do promocji, tak
2509 aby terminal można było promować i rozpocząć przełączanie. W czasie tego procesu węzeł, który nie może
2510 osiągnąć istniejącego przełączenia może wysłać PNPDU wymagane do promocji, tak aby terminal można
2511 było promować i aby rozpoczął on działanie jako przełączenie. W czasie tego procesu terminal odbierze
2512 jednostki PNPDU i wedle własnego uznania wygeneruje pakiety kontrolne PRO_REQ do węzła
2513 podstawowego.

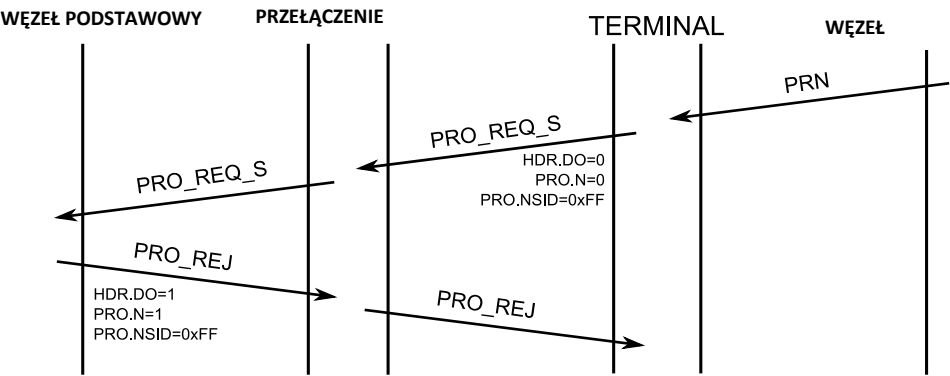
2514 Węzeł podstawowy rozpatruje żądania promocji w czasie ustalonego okresu czasu. Może on użyć adresu
2515 nowego terminala, dostarczonego w pakiecie żądania promocji, aby zdecydować czy zaakceptować
2516 promocję czy nie. Podejmie on decyzję, który węzeł powinien być promowany, jeśli w ogóle, za pomocą
2517 odpowiedzi na promocję. Inne węzły nie odbiorą żadnych odpowiedzi na żądania promocji, aby uniknąć
2518 nasycenia podsieci. Węzeł podstawowy może ewentualnie wysłać odrzucenie, jeśli wystąpi szczególna
2519 sytuacja. Jeżeli podsieć jest specjalnie skonfigurowany, węzeł podstawowy może wysłać żądanie promocji
2520 węzła terminala bezpośrednio do węzła terminala.

2521 Gdy węzeł terminala wymaga promocji, pole PRO.NSID w komunikacie PRO_REQ_S należy wysłać to
2522 wszystkich 1-nek. Pole PRO.NSI powinno zawierać identyfikator LSID przypisany do promowanego węzła w
2523 komunikacie PRO_REQ_B. Zatwierdzający węzeł przełączający powinien ustawić pole PRO.NSID w PRO_ACK
2524 nowo przypisanemu identyfikatorowi LSID. Ten ostateczny PRO_ACK powinien być stosowany przez
2525 pośrednie węzły przełączające do aktualizacji ich tablic przełączania, jak opisano w punkcie 4.3.5.2.

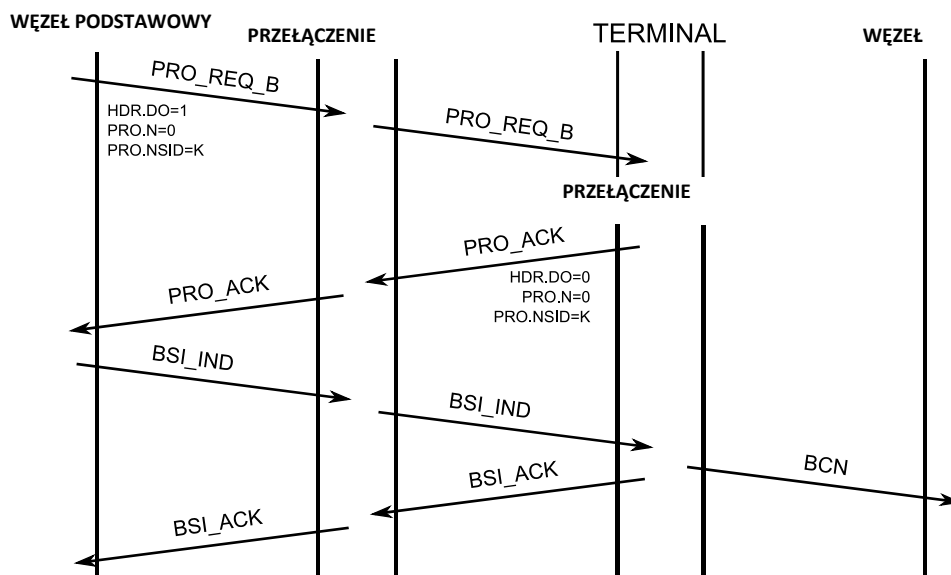
2526 Podczas ponownego stosowania LSID, które zostały uwolnione przez proces degradacji, węzeł podstawowy
2527 nie powinien przydzielać LSID aż do upływu $(macMaxCt/ReTx + 1) * macCt/ReTxTimer$ sekund, aby zapewnić,
2528 że wszystkie pakiety retransmisji, które mogły stosować LSID opuściły podsieć. Podobnie węzeł
2529 podstawowy nie powinien ponownie używać LNID uwolnionego przez proces Utrzymywania aktywności do
2530 czasu upływu T_{keep_alive} sekund za pomocą ostatniej znanej zatwierdzonej wartości T_{keep_alive} , lub jeśli
2531 większa, ostatniej niezatwierdzonej wartości T_{keep_alive} , dla węzła serwisowego za pomocą LNID.



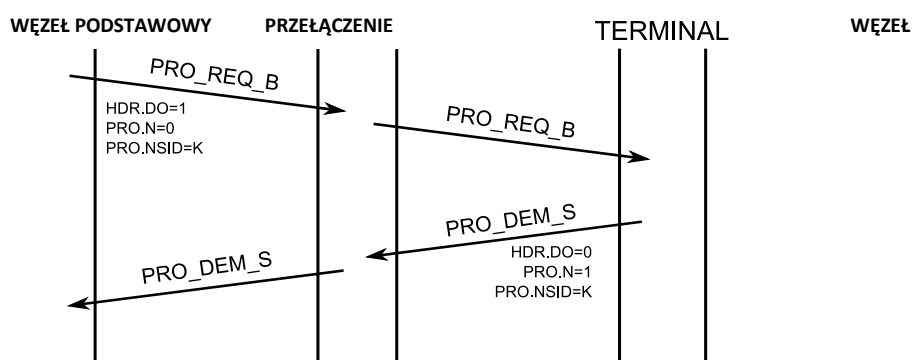
Rys. 63 – Proces promocji inicjowany przez węzeł serwisowy



Rys. 64 – Proces promocji odrzucony przez węzeł podstawowy



Rys. 65 – Proces promocji inicjowany przez węzeł podstawowy



Rys. 66 – Proces promocji odrzucony przez węzeł serwisowy

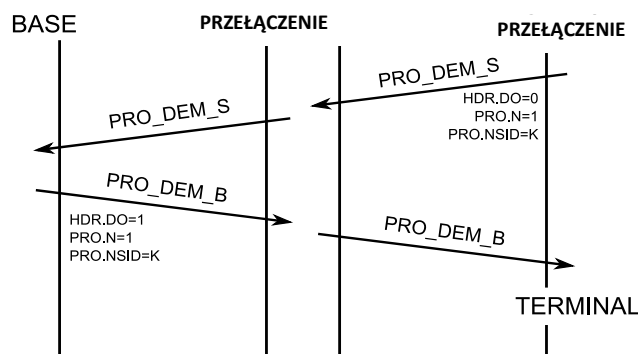
4.6.4 Proces degradacji

Węzeł podstawowy lub węzeł przełączający może w dowolnym momencie zdecydować o zaprzestaniu przełączania. Proces degradacji przewiduje taki mechanizm. Pakiet kontrolny PRO stosowany jest do wszystkich transakcji degradacji.

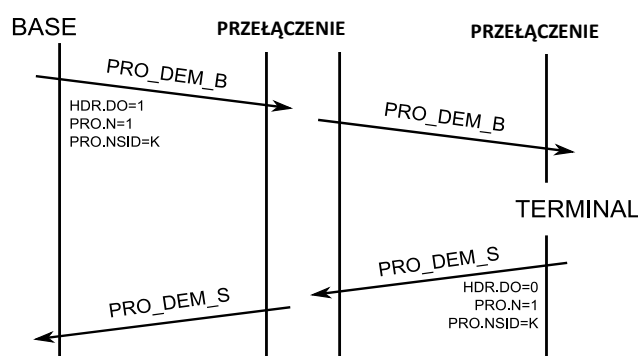
Pole PRO.NSID powinno zawierać SID węzła przełączającego, który jest degradowany jako część transakcji degradacji. Pole PRO.PNA nie jest stosowane w żadnej transakcji procesu degradacji, a jego treść nie jest interpretowana na żadnym końcu.

Po skutecznym zakończeniu procesu degradacji węzeł przełączający powinien natychmiast przerwać przesyłanie sygnałów i zmienić się ze stanu funkcjonalnego *Przełączenie* do stanu *Terminal*. Węzeł podstawowy może realokować LSID i szczelinę sygnału wykorzystywane przez zdegradowane przełączenie po $(macMaxCtIReTx + 1) * macCtIReTxTimer$ sekundach na inne węzły terminala wymagające promocji.

Aktualna wersja specyfikacji nie podaje żadnych wyraźnych informacji na temat odrzucania żądania degradacji przez jednostkę równorzędną na drugim końcu.



Rys. 67 – Proces degradacji inicjowany przez węzeł serwisowy



Rys. 68 – Proces degradacji inicjowany przez węzeł podstawowy

4.6.5 Proces utrzymania aktywności

Proces utrzymania aktywności stosowany jest do wykrywania kiedy węzeł serwisowy opuścił podsieć z powodu zmian w konfiguracji sieci lub z powodu błędów krytycznych, których nie można naprawić.

Gdy węzeł serwisowy odbierze pakiet REG_RSP, korzysta on z pola REG.TIME do uruchomienia zegara T_{keep_alive} . Dla każdego odebranego AL_B zegar jest zerowany za pomocą wartości z ALV.TIME. Powinien on również wysłać ALV_S do węzła podstawowego. Jeśli czas zegara nigdy nie upływa, węzeł serwisowy zakłada, że został on wyrejestrowany przez węzeł podstawowy. Komunikat PRO_REQ również resetuje zegar Keep-Alive do wartości PRO.TIME.

Każde przełączenie wzdłuż ścieżki komunikatu ALV_B powinno przechowywać kopię PRO.TIME oraz ALV.TIME dla każdego węzła przełączającego znajdującego się niżej w strukturze drzewiastej. Jeśli przełączenie nie odbierze komunikatu ALV_S z węzła serwisowego pod nim przez czas T_{keep_alive} określony w PRO.TIME i ALV.TIME, powinien on usunąć pozycję węzła przełączającego z tablicy przełączania. Informacje na temat tablicy przełączania można znaleźć w punkcie 4.3.5.2. Dodatkowo węzeł przełączający może korzystać z REG.TIME i ALV.TIME do rozważenia również statusu rejestracji węzła serwisowego i uwzględnienia go w tablicy przełączania.

Dla każdego komunikatu ALV_B lub ALV_S wysłanego przez węzeł serwisowy lub węzeł podstawowy licznik ALV.TXCNT powinien się zwiększyć przed wysłaniem komunikatu. Licznik ten ma się zawijać. Dla każdego komunikatu ALV_B lub ALV_S odebranego przez węzeł serwisowy lub węzeł podstawowy licznik ALV.RXCNT powinien się zwiększyć. Oczekuje się, że ten licznik również będzie się zawijać. Te dwa liczniki są umieszczane w komunikatach ALV_S and ALV_B. Węzeł podstawowy powinien rozdzielać liczniki ALV.TXCNT i ALV.RXCNT dla każdego węzła serwisowego. Te liczniki są zerowane w procesie rejestracji.

2579

2580 W niniejszej specyfikacji nie opisano algorytmu używanego przez węzeł podstawowy do ustalania kiedy
 2581 należy wysłać komunikaty ALV_B do zarejestrowanych węzłów serwisowych oraz do ustalania wartości
 2582 ALV.TIME i REG.TIME.

2583 4.6.6 Zarządzanie połączeniami

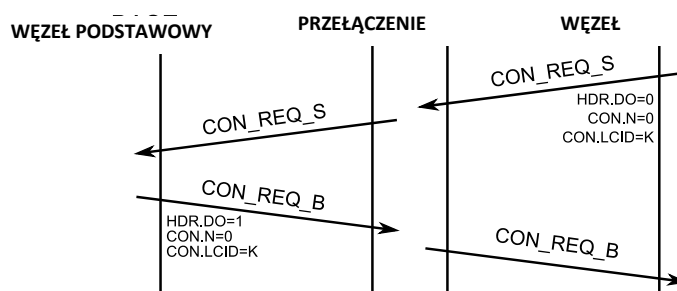
2584 4.6.6.1 Ustawianie połączenia

2585 Ustawianie połączenia działa od końca do końca, łącząc warstwy aplikacji komunikujących się urządzeń.
 2586 W związku z topologią struktury drzewiastej większość połączeń w podsieci będzie miała węzeł podstawowy
 2587 na jednym końcu oraz węzeł serwisowy na drugim. Jednakże, mogą występować przypadki, gdy dwa węzły
 2588 serwisowe w podsieci muszą ustanawiać połączenia. Takie połączenia nazywane są połączeniami
 2589 bezpośrednimi i są opisane w rozdziale 4.3.6.

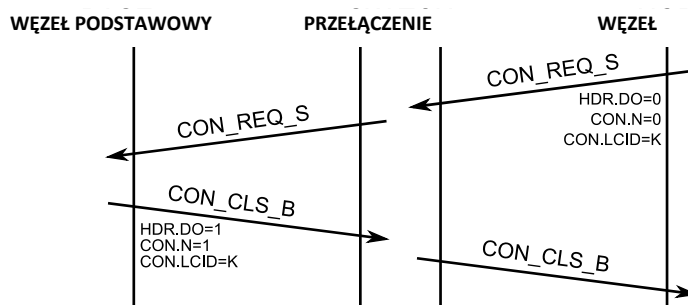
2590 Wszystkie komunikaty dotyczące ustanawiania połączenia korzystają z pakietu kontrolnego CON. W Tabeli
 2591 17 podano różne typy pakietów kontrolnych i określone pola, które je jednoznacznie identyfikują.

2592 Każdemu skutecznemu połączeniu ustanawianemu w podsieci przypisywany jest LCID. Węzeł podstawowy
 2593 powinien przypisać LCID, który jest unikalny dla danego LNID.

2594 **Uwaga:** Dowolny z negocjujących końców może zdecydować o odrzuceniu żądania ustanawiania
 2595 połączenia. Odebranie odrzucenia połączenia nie stanowi żadnych ograniczeń w dokonywaniu przyszłych
 2596 żądań połączenia, może to być jednak wskazane.



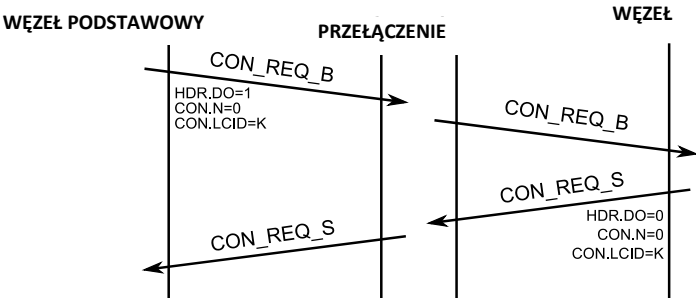
Rys. 69 – Ustawianie połączenia inicjowane przez węzeł serwisowy



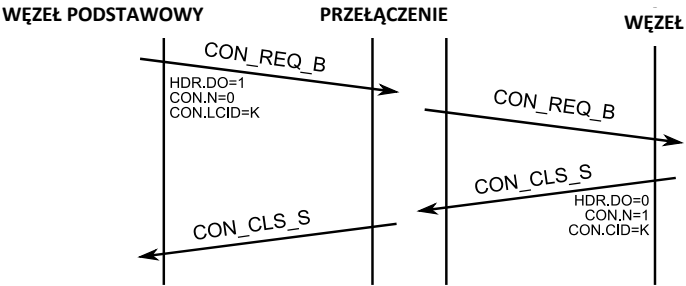
Rys. 70 – Ustawianie połączenia odrzucone przez węzeł podstawowy

2597
 2598

2599
 2600



Rys. 71 – Ustawianie połączenia inicjowane przez węzeł podstawowy



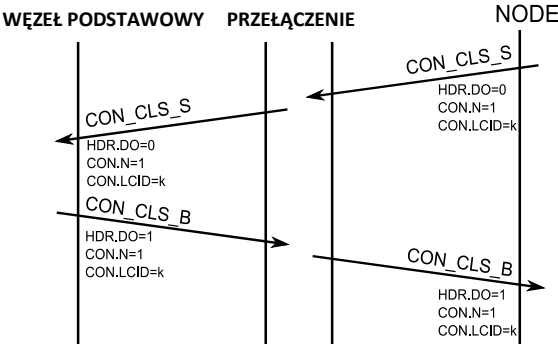
Rys. 72 – Ustawianie połączenia odrzucone przez węzeł serwisowy

4.6.6.2 Zamykanie połączenia

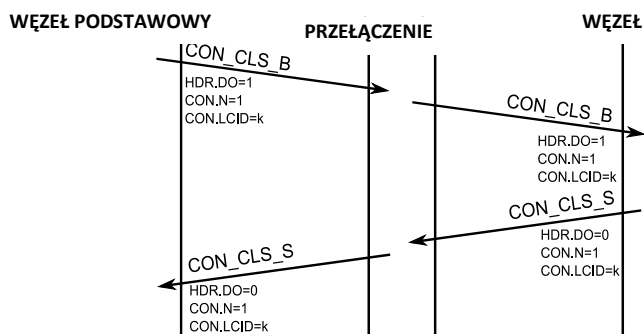
Każda równorzędna jednostka na obu końcach połączenia może zdecydować o zamknięciu połączenia w dowolnym momencie. Pakiet kontrolny CON stosowany jest dla wszystkich komunikatów wymienianych w procesie zamykania połączenia. Jedynie pole CON.N w pakiecie kontrolnym CON ma znaczenie podczas zamykania aktywnego połączenia.

Żądanie zamknięcia połączenia z jednego końca jest potwierdzane przez drugi koniec przed uznaniem połączenia za zamknięte. Aktualna wersja specyfikacji nie podaje żadnych wyraźnych informacji na temat odrzucania zakończenia połączenia wymaganego przez jednostki równorzędne na drugim końcu.

Błąd! Nie można odnaleźć źródła odwołania. i Błąd! Nie można odnaleźć źródła odwołania. pokazują sekwencje wymiany komunikatów w procesie zamykania połączenia.



Rys. 73 – Rozłączanie inicjowane przez węzeł serwisowy



Rys. 74 – Rozłączanie inicjowane przez węzeł podstawowy

4.6.7 Zarządzanie grupą multicast

4.6.7.1 Ogólne

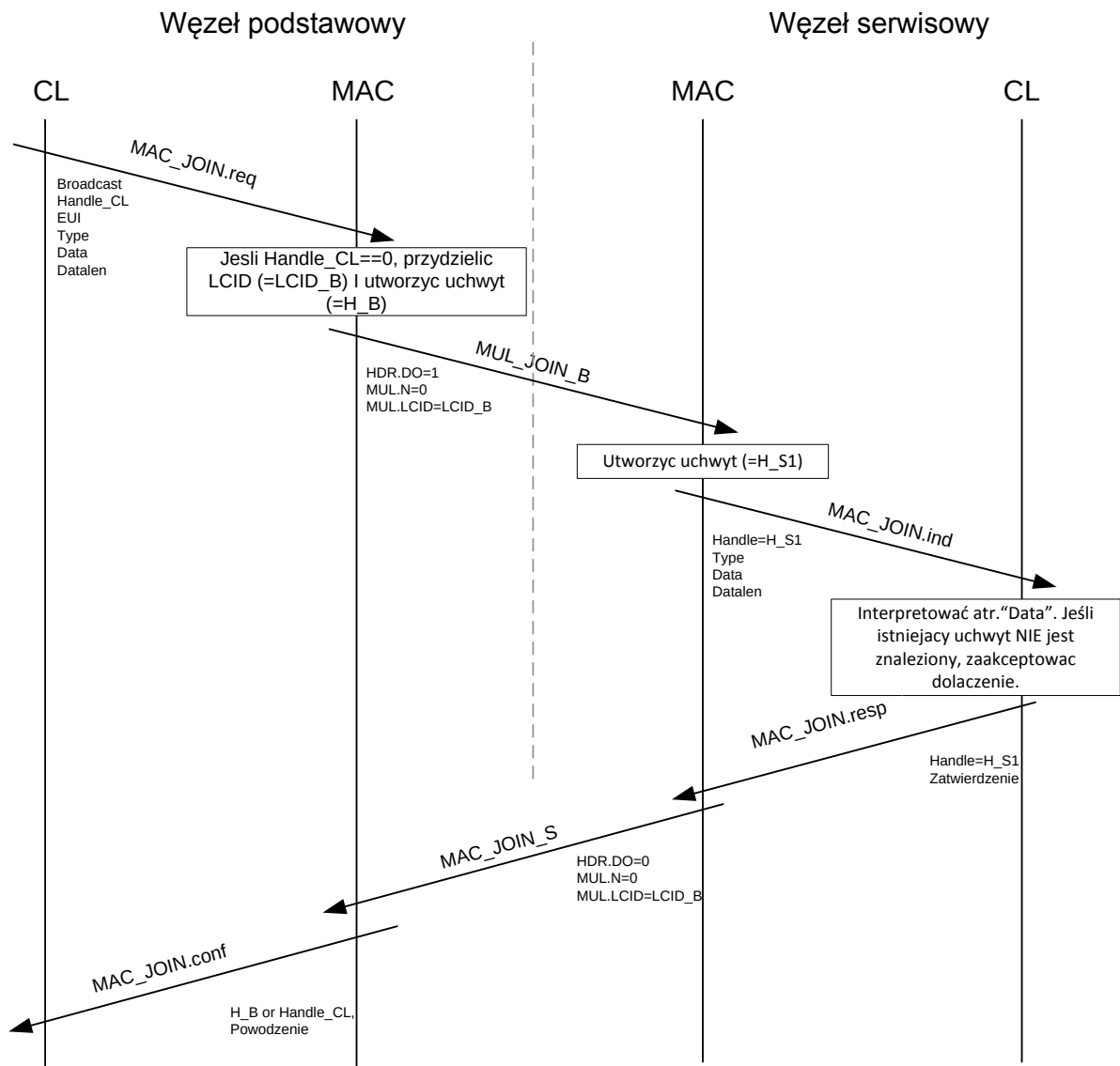
Dołączanie i opuszczanie grupy multicast może zostać zainicjowane przez węzeł podstawowy lub przez węzeł serwisowy. Pakiet kontrolny MUL stosowany jest dla wszystkich komunikatów skojarzonych z multicast, a dla pakietów kontrolnych stosowany jest standardowy mechanizm retransmisji. Te komunikaty kontrolne są transmitowane jako unicast pomiędzy węzłem podstawowym, a węzłem serwisowym.

4.6.7.2 Dołączanie do grupy

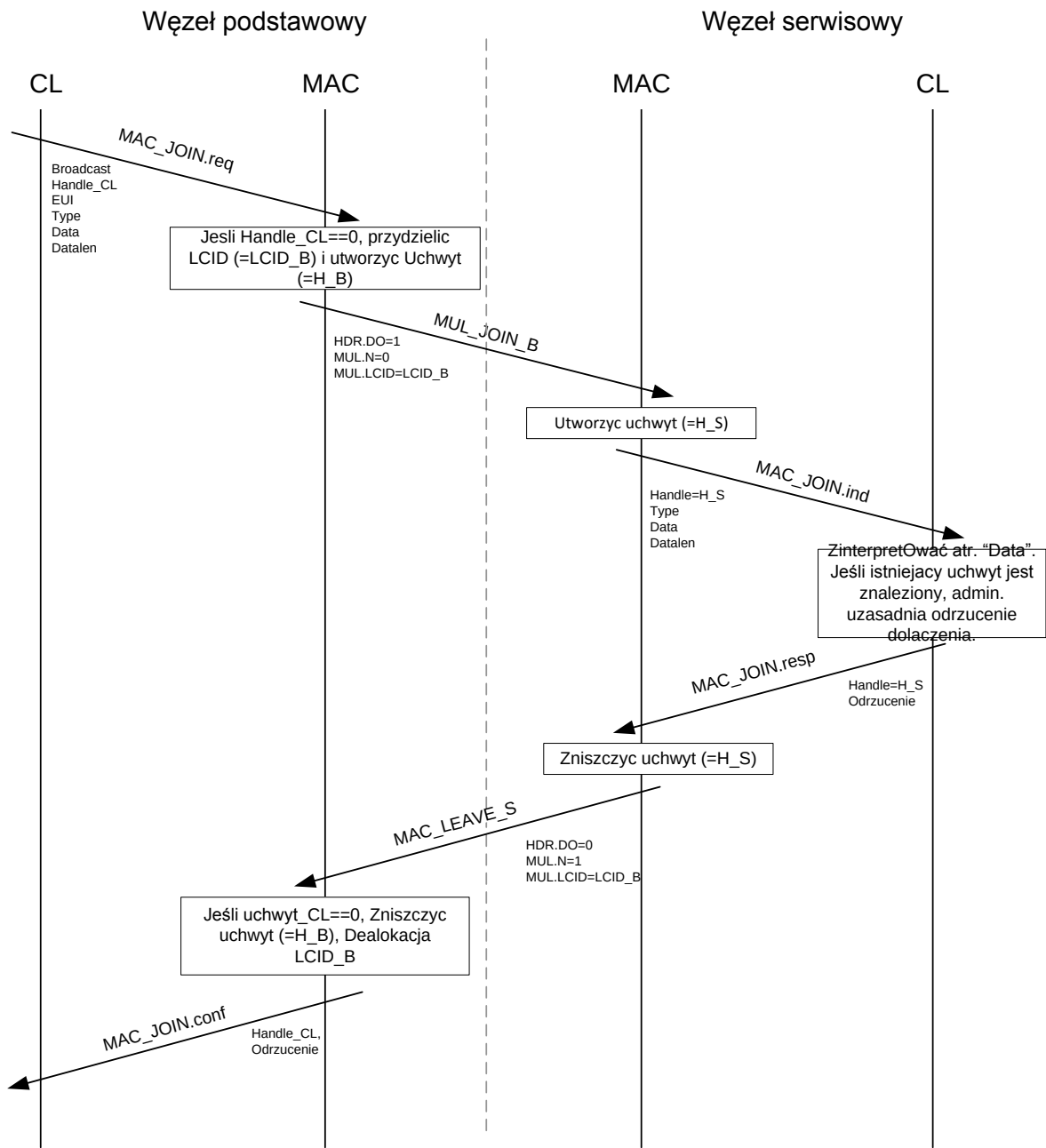
Dołączenie do grupy multicast może zostać zainicjowane z węzła podstawowego lub z węzła serwisowego. Urządzenie nie może rozpocząć procedury nowego dołączania przed ukończeniem istniejącej samoczynnie rozpoczętej procedury dołączania.

Niektóre aplikacje mogą wymagać, aby węzeł podstawowy selektywnie zapraszał określone węzły serwisowe do dołączenia do określonej grupy multicast. W takich przypadkach węzeł podstawowy rozpoczyna nową grupę i zaprasza węzły serwisowe zgodnie z wymaganiami aplikacji.

Skuteczne i nieudane dołączenie do grupy zainicjowane przez Węzeł podstawowy pokazano na Rys. 75 i Rys. 76

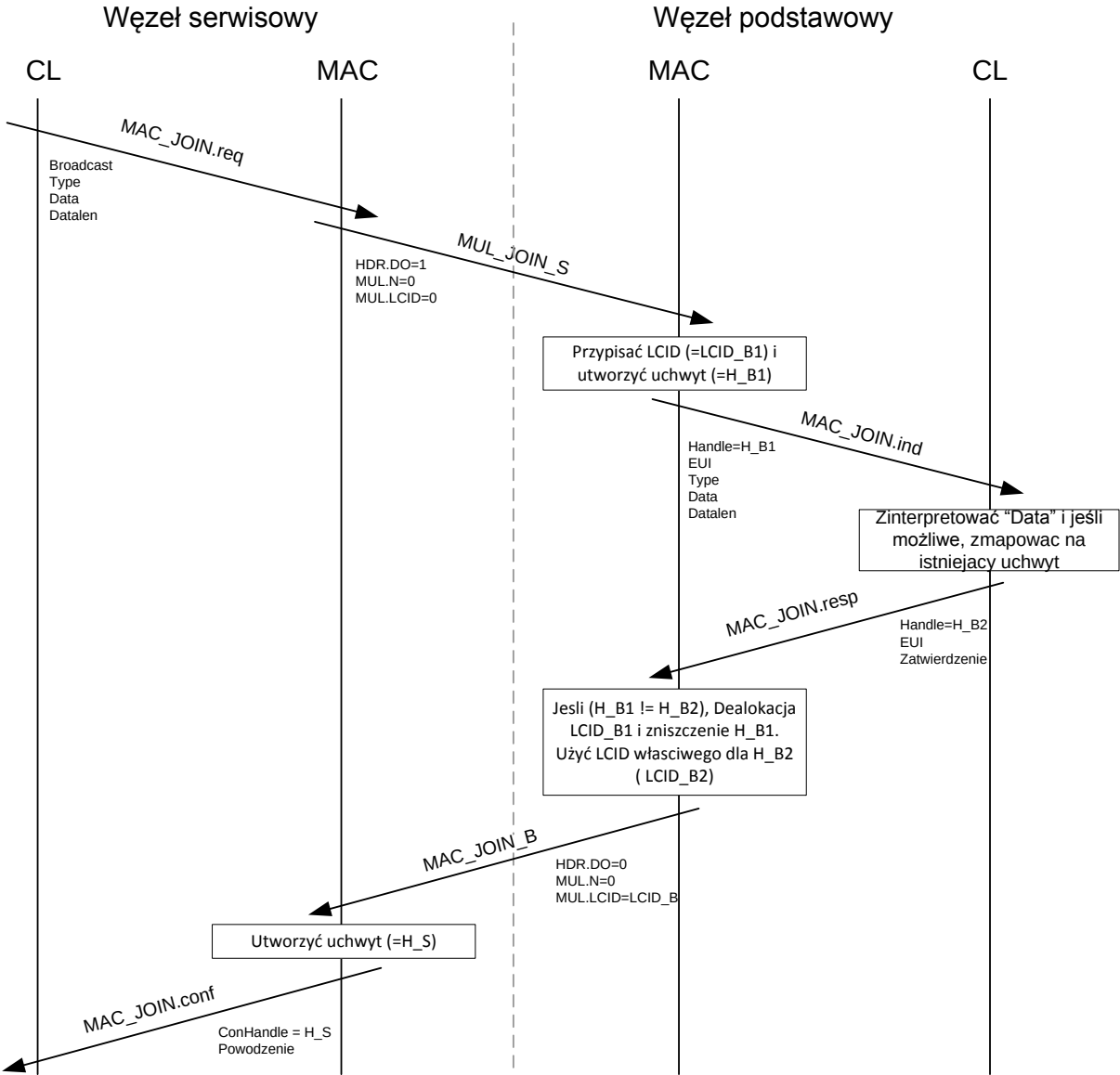


Rys. 75 – Udane dołączenie do grupy inicjowane przez węzeł podstawowy

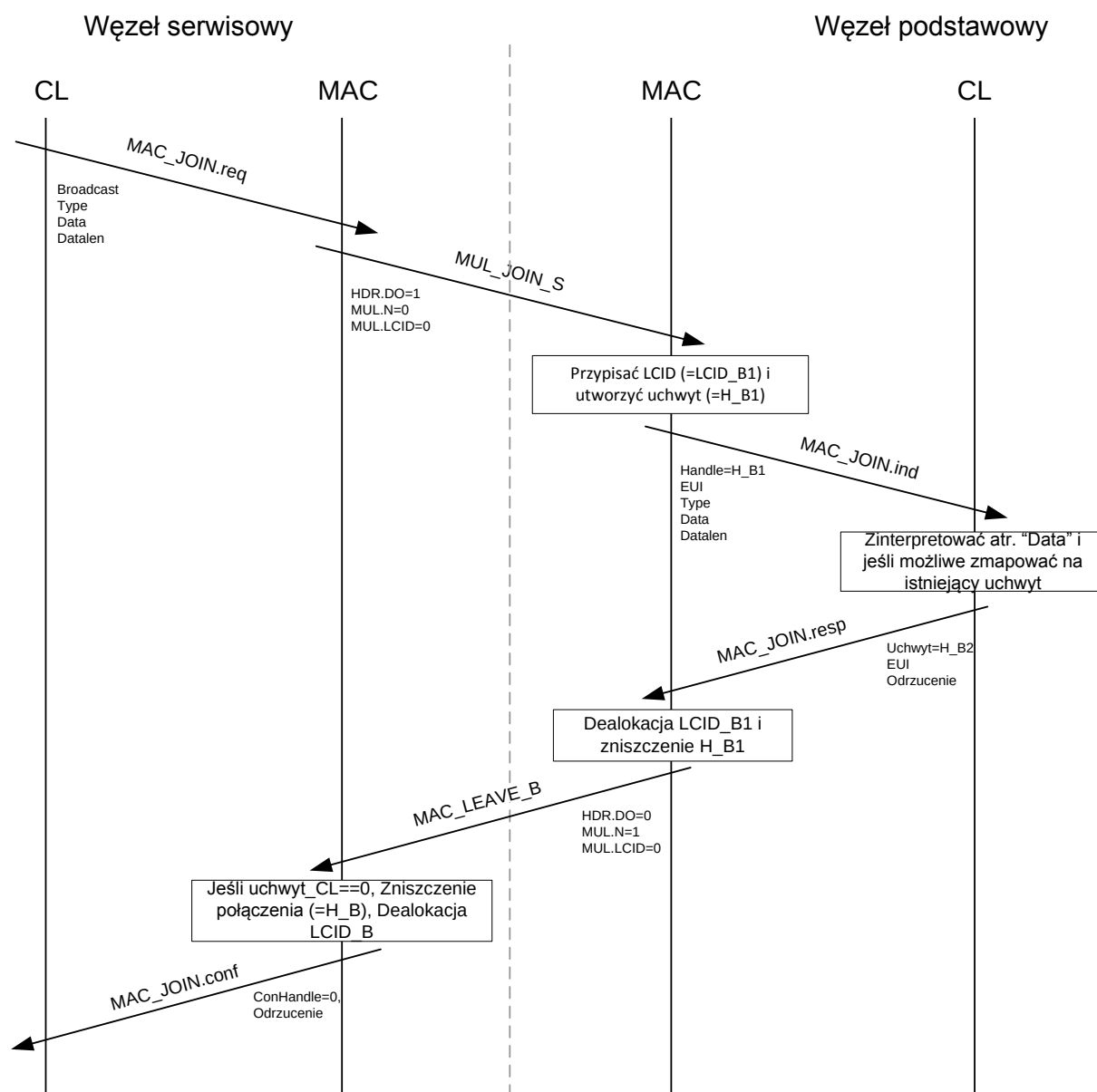


Rys. 76 – Nieudane dołączenie do grupy inicjowane przez węzeł podstawowy

Skuteczne i nieudane dołączenie do grupy zainicjowane przez Węzeł serwisowy pokazano na Rys. 77 i Rys. 78



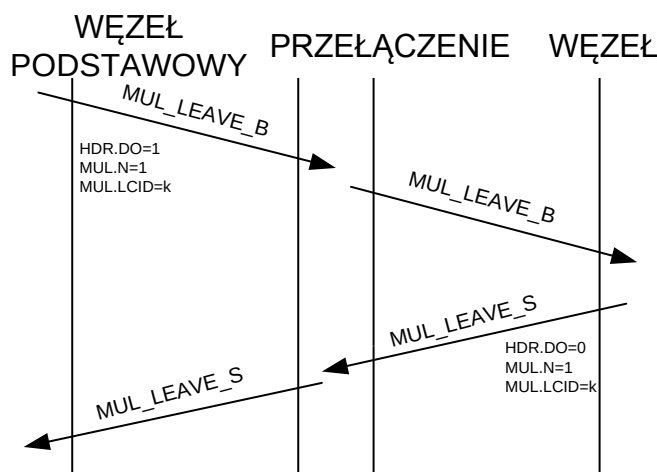
Rys. 77 – Udane dołączenie do grupy inicjowane przez węzeł serwisowy



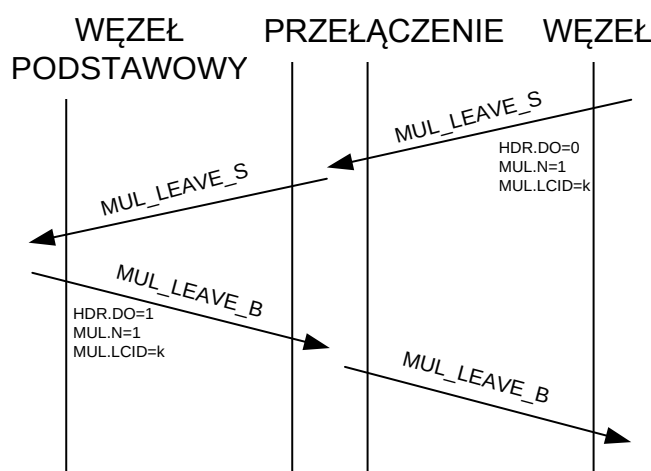
Rys. 78 – Nieudane dołączenie do grupy inicjowane przez węzeł serwisowy

4.6.7.3 Opuszczanie grupy

Opuszczanie grupy multicast działa w taki sam sposób, jak usuwanie połączenia. Albo węzeł podstawowy, albo węzeł serwisowy może zdecydować o opuszczeniu grupy. Istotną różnicą w procesie opuszczania grupy w porównaniu do dołączania do grupy jest brak sekwencji komunikatu dla odrzucania żądania opuszczenia grupy.



Rys. 79 – Opuszczenie grupy inicjowane przez węzeł serwisowy



Rys. 80 – Opuszczenie grupy inicjowane przez węzeł serwisowy

4.6.8 Zarządzanie odpornością warstwy PHY

4.6.8.1 Ogólne

Warstwa PHY ma kilka parametrów, które wpływają na działanie transmisji: przesyłanie energii elektrycznej, schemat modulacji (mapowanie konstelacji i kodowanie splotowe). Nadajnik wymaga informacji zwrotnych na temat jakości odbioru, aby dostosować swoje parametry przesyłowe. Informacje zwrotne są wysyłane przy użyciu pakietów kontrolnych RPM.

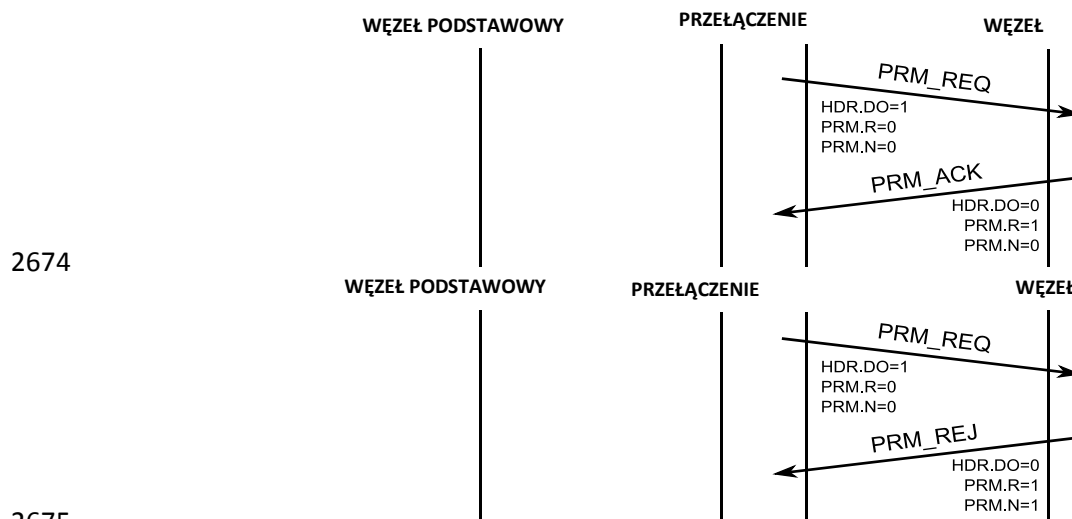
4.6.8.2 Wykrywanie konieczności powiadomienia o odporności warstwy PHY

Dostępne jest kilka źródeł informacji, które mogą mieć zastosowanie do wykrywania czy odporność warstwy PHY jest prawidłowa, czy nie:

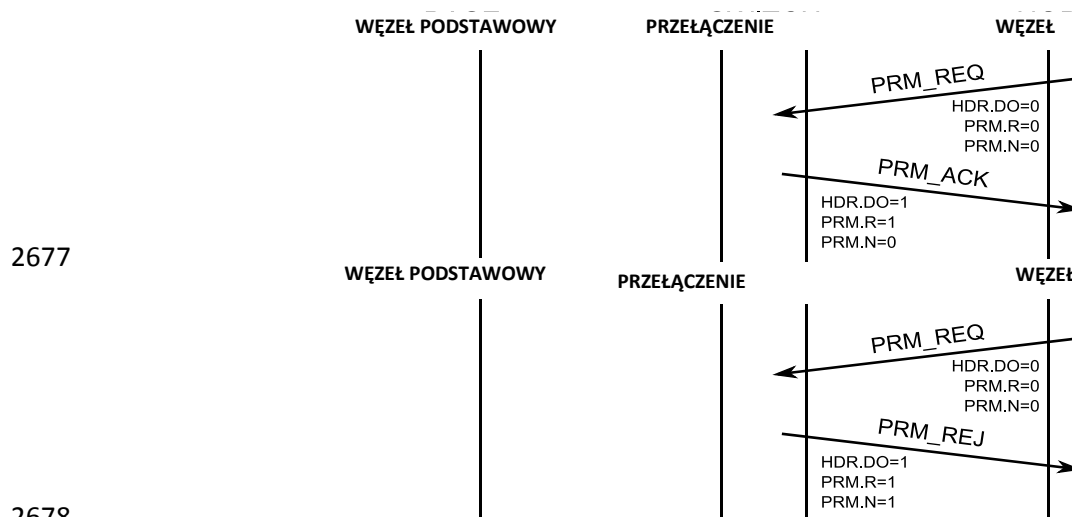
- Odebrano pakiety z nieprawidłową CRC.
- Retransmisje ARQ.
- Retransmisje pakietu kontrolnego.
- Żądania PRM wysłane przez inne węzły od tego samego węzła przełączającego (w przypadku powiadomień węzeł-przełączenie).
- Odpowiedzi PRM.

Te informacje mogą być wykorzystane w celu ustalenia terminu powiadomienia, że odporność warstwy PHY powinna zostać zmieniona. To powiadomienie może zostać przeprowadzone z węzła serwisowego do węzła przełączającego oraz odwrotnie. W tym celu węzeł podstawowy działa jako przełączenie główne, w dokładnie taki sam sposób jak robią to inne węzły przełączające.

4.6.8.3 Powiadomienie o odporności warstwy PHY



Rys. 81 – Zarządzanie odpornością warstwy PHY wnioskowane przez węzeł przełączający



Rys. 82 – Zarządzanie odpornością warstwy PHY wnioskowane przez węzeł serwisowy

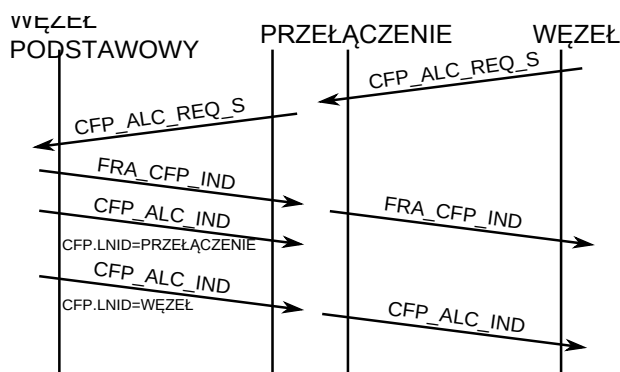
4.6.8.4 Zmiana odporności warstwy PHY

Z punktu widzenia warstwy PHY istnieje kilka parametrów, które należy dostosować i które wpływają na odporność transmisji: moc transmisji i parametry modulacji (szyfrowanie slotowe i konstelacja). Co do zasady, należy przestrzegać następujących zasad:

- **Zwiększanie odporności:** zwiększanie mocy, a jeśli nie jest to możliwe, usprawnianie odporności schematu modulacji (redukcja przepustowości).
- **Zmniejszanie odporności:** zmniejszanie odporności schematu modulacji (zwiększanie przepustowości), a jeśli nie jest to możliwe, redukcja mocy transmisji.

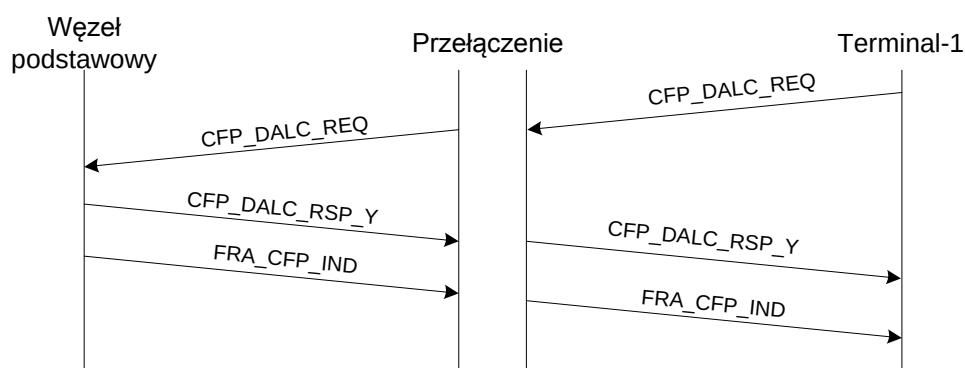
4.6.9 Alokacja i dealokacji kanału

Rys. 83 pokazuje sekwencję skutecznej alokacji kanału. Wszystkie żądania przydziału kanału są przekazywane do węzła podstawowego. Należy zauważyć, że w celu zapewnienia bezkolizyjnej alokacji kanału wzdłuż całej ścieżki, węzeł podstawowy przydziela do pośrednich węzłów przełączających czasy niepokrywające się. W sieci wielopoziomowej węzeł podstawowy może również ponownie wykorzystać przydzielony czas na różnych poziomach. Przy ponownym korzystaniu ze wspomnianego czasu, węzeł podstawowy musi zapewniać, że poziomy, które korzystają z tych samych szczelin czasu są dostatecznie rozdzielone, aby zapobiec możliwym zakłóceniom.



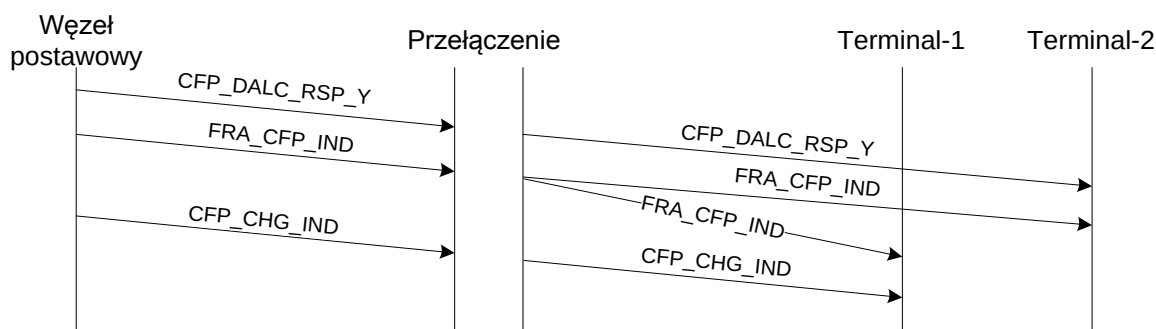
Rys. 83 – Skuteczna alokacja okresu CFP

Rys. 84 poniżej pokazuje żądanie dealokacji kanału z Terminala i wynikowe potwierdzenie Węzła podstawowego.



Rys. 84 – Sekwencja skutecznej dealokacji kanału

Rys. 85 poniżej pokazuje sekwencję zdarzeń, które mogą prowadzić do realokacji przez węzeł podstawowy bezkolizyjnej szczeliny do Terminala, który już ma przydzielone do niego szczeliny. W tym przykładzie żądanie dealokacji z Terminala 2 doprowadziło do dwóch zmian: po pierwsze w globalnej strukturze ramki - zmiana ta przekazywana jest do podsieci w pakiecie FRA_CFP_IND; po drugie jest ona właściwa dla szczeliny czasu przypisanej do Terminala 1 w okresie bezkolizyjnego dostępu.



Rys. 85 – Dealokacja kanału do jednego urządzenia prowadzi do zmiany okresu CDP przydzielonego do innego urządzenia

4.7 Automatyczne żądanie powtórzenia (ARQ)

4.7.1 Ogólne

Urządzenie spełniające wymagania tej specyfikacji może albo wdrożyć schemat ARQ jak opisano w niniejszym punkcie lub wcale nie używać ARQ. Niniejsza specyfikacja zapewnia niskokosztowe urządzenia przełączające i terminalowe, które nie wdrażają żadnych mechanizmów ARQ.

4.7.2 Początkowe negocjowanie

ARQ jest właściwością połączenia. W czasie wstępnych negocjacji połączeń inicjujące urządzenie wskazuje, czy woli, aby w polu CON.ARQ występowało automatyczne żądanie powtórzenia, czy nie. Urządzenie odpowiadające na drugim końcu może wskazywać przyjęcie lub odrzucenie przez niego ARQ w odpowiedzi. Jeśli oba urządzenia zgadzają się korzystać z ARQ dla połączenia, cały ruch w połączeniu będzie stosować ARQ do zatwierdzeń, jak opisano w punkcie 4.7.3. Jeśli urządzenie odpowiadające odrzuci ARQ w tej odpowiedzi, dane przepływające przez to połączenie nie będą stosować ARQ.

4.7.3 Mechanizm ARQ

4.7.3.1 Ogólne

Mechanizm ARQ działa pomiędzy bezpośrednio podłączonymi urządzeniami równorzędnymi (oryginalne źródło i ostateczne urządzenie docelowe), tak długo jak oba z nich obsługują wdrażanie ARQ. Oznacza to, że nawet w przypadku połączenia pomiędzy węzłem podstawowym a terminalem (podłączonym za pośrednictwem jednego lub większej liczby pośrednich urządzeń przełączających) ARQ działa na zasadzie „od końca do końca”. Zachowanie węzłów przełączających w połączeniu włączonym przez ARQ opisano w punkcie 4.7.4. Podczas korzystania z ARQ, unikalny identyfikator pakietu kojarzony jest z każdym pakietem, aby pomóc w zatwierdzeniu. Identyfikator pakietu ma długość 6 bitów i może tym samym oznaczać 64 różne pakiety. Okienkowanie ARQ jest obsługiwane przy maksymalnym rozmiarze okna 32 (5 bitów), jak opisano w punkcie 4.7.3.3.

4.7.3.2 ARQ PDU

4.7.3.2.1 Ogólne

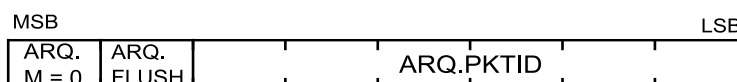
Podnagłówek ARQ umieszczany jest w pakietach danych po nagłówku pakietu i przed ORYGINALNĄ treścią pakietu:

Ogólny nagłówek MAC	Podnagłówek ARQ	Treść pakietu
---------------------	-----------------	---------------

Rys. 86 - PDU danych warstwy MAC z podnagłówkiem ARQ

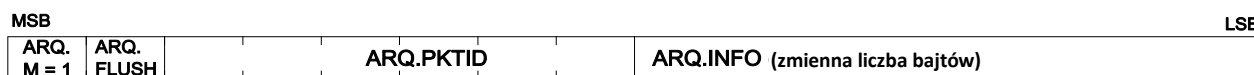
W przypadku ARQ PDU pole PKT.LEN w nagłówku pakietu będzie ustawione jako długość podnagłówka ARQ plus długość oryginalnej treści pakietu. W ten sposób pośredni węzeł przełączający może prawidłowo rozbić całą długość PDU bez wiedzy, że ta jednostka PDU ma włączone ARQ, więc może w jasny sposób przekazywać PDU ARQ na podstawie samych informacji o adresowaniu.

Podnagłówek ARQ zawiera zestaw bajtów, w którym każdy bajt zawiera różne podpola. Najbardziej znaczący bit każdego bajta, bit M, wskazuje, czy w nagłówku ARQ jest więcej bajtów.



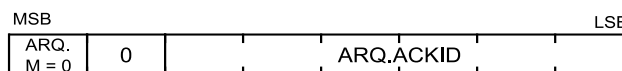
Rys. 87 - Podnagłówek ARQ jedynie z identyfikatorem pakietu

Rys. 87 pokazuje podnagłówek ARQ z pierwszym M bitem z 0, a więc podnagłówek jest pojedynczym bajtem i zawiera jedynie identyfikator pakietu dla przesyłanego pakietu.

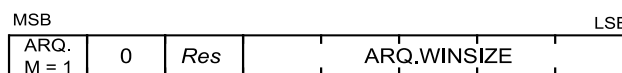


Rys. 88 - Podnagłówek ARQ z ARQ.INFO

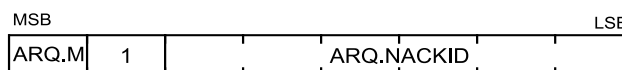
Rys. 88 ma M bitów w pierwszym bajcie podnagłówka, a zatem podnagłówek zawiera wiele bajtów. Pierwszy bajt zawiera identyfikator pakietu przesyłanego pakietu, a po nim następuje ARQ.INFO, który jest listą o długości jednego lub więcej bajtów, gdzie każdy bajt może mieć następujące znaczenie:



Rys. 89 - Pola bajta ARQ.ACK



Rys. 90 - Pola bajta ARQ.WIN



Rys. 91 - Pola bajtów ARQ.NACK

Jeśli istnieje wiele utraconych pakietów, ARQ.NACK jest wysyłane do każdego z nich, od pierwszego utraconego pakietu do ostatniego utraconego pakietu. Jeśli istnieje kilka ARQ.NACK, zatwierdzone są pakiety przed pierwszym ARQ.NACK oraz pakiety przed brakiem zatwierdzenia ARQ.NACK. W przypadku występowania zatwierdzenia - ARQ.ACK, należy go umieścić na końcu podnagłówka ARQ i powinien się on odnosić do identyfikatora ARQ.ACKID występującego po dowolnym identyfikatorze ARQ.NACKID (jeśli taki występuje). Jeśli występuje co najmniej jeden brak zatwierdzenia ARQ.NACK i jedno zatwierdzenie ARQ.ACK, każdy pakiet pomiędzy ostatnim brakiem zatwierdzenia ARQ.NACKID i ARQ.ACK zostaje zatwierdzony.

2769 Dla celów interoperacyjności, urządzenie powinno być w stanie odbierać wszelkie dobrze utworzone
 2770 podnagłówki ARQ i powinno przetwarzać co najmniej pierwsze pole ARQ.ACK lub ARQ.NACK.

2771 Podpola mają następujące znaczenie jak opisano w Tabeli 51

2772 **Tabela 51 - Pola ARQ**

Pole	Opis
ARQ.FLUSH	ARQ.FLUSH = 1 jeśli zatwierdzenie ACK musi być wysłane natychmiast. ARQ.FLUSH = 0 jeśli zatwierdzenie ACK nie jest wymagane.
ARQ.PKTID	Identyfikator bieżącego pakietu - jeśli pakiet jest pusty (bez jakichkolwiek danych), jest to identyfikator pakietu, który będzie wysłany w następnej kolejności.
ARQ.ACKID	Identyfikator kolejnego oczekiwanego do odbioru pakietu.
ARQ.WINSIZE	Rozmiar okna dostępny w ostatnim zatwierdzonym pakiecie. Po nawiązaniu połączenia jego okno to 1.
ARQ.NACKID	Identyfikatory pakietów, które należy przesłać ponownie.

2773 4.7.3.2.2 Przykład podnagłówka ARQ

MSB	ARQ. M = 1	ARQ. FLUSH = 1	ARQ.PKTID = 23	ARQ. M = 1	0	Res	ARQ.WINSIZE = 16	LSB
ARQ. M = 1	1		ARQ.NACKID = 45	ARQ. M = 1	1		ARQ.NACKID = 47	
ARQ. M = 1	1		ARQ.NACKID = 48	ARQ. M = 1	1		ARQ.NACKID = 52	
ARQ. M = 1	1		ARQ.NACKID = 55	ARQ. M = 1	1		ARQ.NACKID = 56	
ARQ. M = 1	1		ARQ.NACKID = 57	ARQ. M = 0	0		ARQ.ACKID = 60	

Rys. 92 - Przykład podnagłówka ARQ z wszystkimi polami

2776 W tym przykładzie obecne są wszystkie pola podnagłówka ARQ. Aby było to zrozumiałe, gdyż oba węzły są
 2777 nadajnikami i odbiornikami, strona odbiorcza tego nagłówka będzie nazwana stroną A, a druga strona
 2778 wysyłająca stroną B. Komunikat posiada identyfikator pakietu 23 jeśli zawiera dane; w przeciwnym razie
 2779 kolejny pakiet do wysłania będzie miał identyfikator danych 23. Ponieważ ustawiony jest bit resetujący,
 2780 musi być on zatwierdzony/niezatwierdzony.

2781 B żąda retransmisji pakietów 45, 47, 48, 52, 55, 56 i 57. ACK = 60, więc strona B odbierała pakiety <45, 46,
 2782 49, 50, 51, 53, 54, 58 i 59.

2783 Okno ma identyfikator nr 16 i odebrało i przetworzyło wszystko do pakietu 44 (pierwszy niezatwierdzony
 2784 NACK=45), więc A może wysłać wszystkie pakiety <= 60, to jest poza wysyłaniem żądanych retransmisji
 2785 może również wysłać pakiet o ID =60.

2786 4.7.3.3 Okienkowanie

2787 Nowe połączenie pomiędzy dwoma urządzeniami równorzędnymi rozpoczyna się od niejawnego
 2788 początkowego rozmiaru okna odbiornika = 1 i identyfikatora pakietu 0. Ten rozmiar okna jest przypadkiem
 2789 ograniczenia, a transakcja(na początek) będzie zachowywać się jak mechanizm ARQ „Stop and Wait”.

2790 Po odebraniu ARQ.WIN nadawca dostosuje swój rozmiar okna do *ARQ.WINSIZE*. Ten rozmiar bufora jest
 2791 liczony od pierwszego całkowicie zatwierdzonego pakietu, więc jeśli występuje lista pozycji
 2792 niezatwierdzonych, a następnie zatwierdzenie, rozmiar okna określa liczbę pakietów od pierwszego pakietu
 2793 niezatwierdzonego, który mógłby zostać wysłany. Jeśli w pakiecie jest tylko zatwierdzenie ACK (bez NACK),
 2794 rozmiar okna określa liczba pakietów, którą można wysłać z tego ACK.

2795 Wartość *ARQ.WINSIZE* równa 0 może zostać przesłana z powrotem przez odbiorcę celem wskazania
 2796 przeciążenia na jej końcu. W takich przypadkach koniec wysyłający powinien odczekać przez co najmniej
 2797 czas *ARQCongClrTime* przed ponowną transmisją danych.

2798 4.7.3.4 Kontrola przepływu

2799 Nadajnik musi zarządzać ACK wysyłającym algorytm przez bit resetujący; od niego zależy prawidłowa
 2800 komunikacja ARQ. Odbiornik zmuszony jest do wysyłania zatwierdzeń ACK jedynie, gdy nadajnik wysłał
 2801 pakiet z ustawionym bitem resetującym, mimo że odbiornik mógł wysłać więcej zatwierdzeń ACK nawet
 2802 jeśli nie był do tego zmuszony, ponieważ kontrola przepływu leży wyłącznie w odpowiedzialności nadajnika.

2803 Są to warunki wstępne dla interoperacyjności, ale algorytm zależy od producenta. Zaleca się, aby nakładać
 2804 informacje na temat danych ACK w pakietach wychodzących, aby uniknąć transmisji niepotrzebnych
 2805 pakietów tylko do zatwierdzania.

2806 4.7.3.5 Zalecenia dotyczące algorytmów

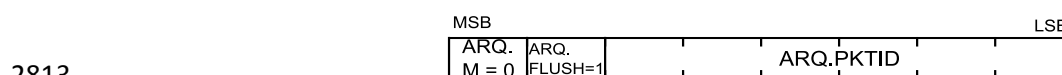
2807 Nie został określony żaden algorytm normatywny, informacje na temat zaleceń można znaleźć w Załącznik I.

2808 4.7.3.6 Stosowanie ARQ w urządzeniach o ograniczonych zasobach

2809 Urządzenia o ograniczonych zasobach mogą mieć małą pamięć i proste wdrożenie ARQ. Mogą one chcieć
 2810 korzystać z okna 1 pakietu. Będą one działać jako mechanizm Stop-and-Wait.

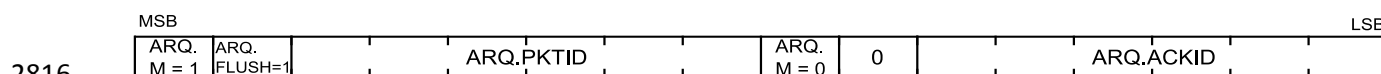
2811 Podnagłówek ARQ do wygenerowania może wyglądać następująco:

2812 Jeśli nie ma nic do zatwierdzenia:



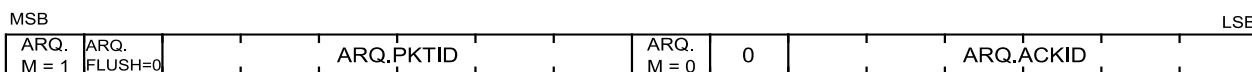
2814 Rys. 93 - Podnagłówek ARQ Stop-and-Wait jedynie z identyfikatorem pakietu

2815 Jeśli istnieją dane do zatwierdzenia:



2817 Rys. 94 - Podnagłówek ARQ Stop-and-Wait z zatwierdzeniem (ACK)

2818 Jeśli istnieje coś do zatwierdzenia, ale pakiet nie zawiera danych:



Rys. 95 - Podnagłówek ARQ Stop-and-Wait bez danych i z ACK

Atrybut ARQ.WINSIZE zazwyczaj nie jest przesyłany ponieważ rozmiar okna domyślnie wynosi już 1. Może być on przesyłany jedynie w celu zarządzania przeciążeniami sieci i wznowianiem transmisji.

4.7.4 Przełączanie pakietów ARQ

Wszystkie węzły przełączające powinny obsługiwać transparentne mostkowanie ruchu ARQ, zarówno jeśli obsługują ARQ dla własnych transmisji i odbiorów. W tym trybie węzły przełączające nie muszą buforować pakietów połączeń ARQ dla retransmisji.

Niektóre węzły przełączające mogą buforować pakiety połączeń ARQ i wykonywać retransmisje w odpowiedzi na brak zatwierdzeń tych pakietów. Należy postępować zgodnie z następującymi zasadami ogólnymi.

- Identyfikatory zatwierdzonych pakietów powinny być spójne od końca do końca.
- Buforowanie pakietów w węzłach przełączających i ich retransmisje powinny być zrozumiałe dla węzłów źródłowych i docelowych, tj. węzeł źródłowy lub docelowy nie musi wiedzieć, czy przełączenie pośrednie buforowało pakiety dla przetaczonych danych czy nie.

5 Warstwa konwergencji

5.1 Omówienie

Rys. 96 pokazuje ogólną strukturę warstwy konwergencji.



2839

2840

Rys. 96 – Struktura warstwy konwergencji

2841 Warstwa konwergencji podzielona jest na dwie podwarstwy. Podwarstwa styku CPCS zapewnia zestaw
 2842 ogólnych usług. Podwarstwa konwergencji właściwa dla usługi (SSCS) zawiera usługi właściwe dla jednego
 2843 profilu komunikacji. Istnieje kilka podwarstw SSCS, zazwyczaj jedna na profil komunikacji, ale tylko jedna
 2844 podwarstwa CPCS. Korzystanie z usług CPCS jest opcjonalne w tym, że niektóre SSCS będą korzystać z usług,
 2845 których wymagają z CPCS i pomijać usługi, które nie są potrzebne.

5.2 Podwarstwa styku CPCS

5.2.1 Ogólne

2848 Ta specyfikacja definiuje jedynie jedną usługę CPCS: Podział i scalanie (SAR).

5.2.2 Podział i scalanie (SAR)

5.2.2.1 Ogólne

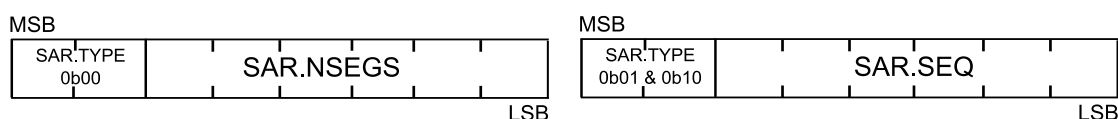
2851 Jednostki SDU podwarstwy styku CPCS które są większe, niż CMTUSize-1 bajtów są dzielone w CPCS.
 2852 Jednostki SDU podwarstwy styku CPCS, które są równe lub mniejsze niż CMTUSize-1 bajtów mogą również
 2853 zostać opcjonalnie podzielone. Podział oznacza rozbić jednostek SDU podwarstwy CPCS na mniejsze części
 2854 do przesłania do warstwy MAC. W równorzędnej podwarstwie CPCS mniejsze części (segmenty) są z
 2855 powrotem scalane, aby utworzyć kompletną jednostkę SDU CPCS. Wszystkie segmenty poza ostatnim
 2856 segmentem podzielonej jednostki SDU muszą mieć ten sam rozmiar i co najmniej CMTUSize bajtów
 2857 długości. Segmenty mogą być ustanawiane jako mniejsze niż „CMTUSize -1” bajtów na przykład., gdy kanał
 2858 jest słaby. Ostatni segment może oczywiście być mniejszy niż CMTUSize-1 bajtów.

Aby utrzymywać prostą funkcjonalność SAR, rozmiar *CIMTUSize* jest stałą wartością dla wszystkich możliwych kombinacji modulacji/kodowania w warstwie PHY. Wartość *CIMTUSize* to wartość występująca kiedy za pomocą kombinacji modulacji/kodowania zawsze możliwe jest wysłanie pojedynczego segmentu w jednej jednostce PPDU. Dlatego nie ma potrzeby odkrywania określonej maksymalnej jednostki transmisyjnej pomiędzy równorzędnymi CPCS lub modyfikowania konfiguracji SAR dla każdej zmiany w kombinacji modulacji/kodowania. W celu zwiększenia wydajności węzeł serwisowy, który obsługuje połączenie pakietów może połączyć wiele segmentów w jedną jednostkę PPDU podczas komunikowania się z węzłem równorzędnym.

Podział zawsze dodaje do każdego segmentu nagłówek 1-bajtowy. Pierwsze dwa bity nagłówka SAR identyfikują typ segmentu. Semantyka reszty informacji nagłówka zależy będzie od typu segmentu. Struktura różnych typów nagłówka pokazana została na Rys. 97, a poszczególne pola wyjaśniono w

Tabela 52.

Nie wszystkie pola są obecne w nagłówku SAR. Obecne jest albo SAR.NSEGS, albo SAR.SEQ, ale nigdy oba z nich.



Rys. 97 - Nagłówki podziału i scalania

Tabela 52 - Pola nagłówka SAR

Nazwa	Długość	Opis
SAR.TYPE	2 bity	Typ segmentu. 0b00: pierwszy segment; 0b01: segment pośredni; 0b10: ostatni segment; 0b11: zarezerwowany w tej wersji specyfikacji.
SAR.NSEGS	6 bitów	'Liczba segmentów' – 1.
SAR.SEQ	6 bitów	Liczba sekwencji segmentu.

Każdy segment (poza pierwszym) obejmuje liczbę sekwencji, tak aby stratę segmentu można było wykryć podczas scalania. Numeracja sekwencji powinna rozpocząć się od zera przy każdej nowej jednostce SDU CPCS. Pierwszy segment, który zawiera pole SAR.SEQ musi mieć wartość SAR.SEQ=0. Wszystkie kolejne segmenty z tej samej jednostki SDU CPCS powinny zwiększać tę liczbę sekwencji, tak aby pole SAR.SEQ dodawało jeden numer przy każdej transmisji.

Wartość SAR.NSEGS wskazuje całkowitą liczbę segmentów minus jeden. Zatem gdy SAR.NSEGS = 0, jednostka SDU CPCS wysyłana jest w jednym segmencie. SAR.NSEGS = 63 wskazuje, że dostępne będą 64 segmenty do utworzenia pełnej jednostki SDU podwarstwy CPCS. Gdy SAR.NSEGS = 0, wskazuje to, że ten

2885 pierwszy segment jest również ostatnim segmentem. Dla tej jednosegmentowej jednostki SDU CPCS nie
2886 przewiduje się kolejnych segmentów z SAR.TYPE = 0b01 lub 0b10.

2887 SAR po stronie odbiorczej powinien buforować wszystkie segmenty i dostarczać jedynie w pełni złożone
2888 jednostki SDU CPCS do podwarstwy SSCS. Jeśli scalanie nie powiedzie się w wyniku nieodebrania segmentu
2889 lub odebrania zbyt wielu segmentów, itd., SAR nie dostarczy żadnych niepełnych jednostek SDU CPCS do
2890 SSCS.

2891 5.2.2.2 Stałe SAR

2892 Tabela 53 pokazuje stałe usługi SAR.

2893 Tabela 53 - Stałe SAR

Stała	Wartość
CIMTUSize	256 bajtów
CIMaxAppPktSize	Maksymalna wartość (SAR.NSEGS) x CIMTUSize.

2894 5.3 Zerowa podwarstwa konwergencji właściwa dla usługi (Zerowa 2895 SSCS)

2896 5.3.1 Omówienie

2897 Zerowa podwarstwa SSCS zapewnia warstwie MAC transparentną, możliwie najprostszą ścieżkę do górnych
2898 warstw i minimalizując narzut. Jest ona przeznaczona do zastosowań, które nie wymagają żadnych
2899 specjalnych zdolności do konwergencji.

2900 Połączenia unicast i multicast tej podwarstwy SSCS powinny korzystać z usługi SAR, tak jak określono to w
2901 punkcie 5.2.2. Jeśli nie potrzebują one usługi SAR, powinny w dalszym ciągu zawierać nagłówek SAR
2902 (powiadamiając jedynie jeden segment).

2903 CON.TYPE i MUL.TYPE (patrz Załącznik E) dla połączeń unicast i grup multicast powinny stosować ten sam
2904 typ, który został już zdefiniowany dla aplikacji wykorzystującej tą zerową podwarstwę SSCS.

2905 5.3.2 Prymitywy

2906 Prymitywy zerowej SSCS są po prostu bezpośrednim mapowaniem prymitywów MAC. Unika się pełnego
2907 opisu każdego prymitywu, ponieważ mapowanie jest bezpośrednie, a prymitywy będą działać tak, jak
2908 prymitywy warstwy MAC.

2909 Bezpośrednio zmapowane prymitywy mają dokładnie te same parametry, jak te w warstwie MAC i
2910 wykonują tą samą funkcjonalność. Zestaw prymitywów, które są mapowane bezpośrednio pokazano
2911 poniżej.

2912

2913

2914

Tabela 54 - Mapowanie prymitywów pomiędzy prymitywami podwarstwy zerowej SSCS a prymitywami warstwy MAC

Zerowa podwarstwa SSCS zmapowana na ...	... prymityw MAC
CL_NULL_ESTABLISH.request	MAC_ESTABLISH.request
CL_NULL_ESTABLISH.indication	MAC_ESTABLISH.indication
CL_NULL_ESTABLISH.response	MAC_ESTABLISH.response
CL_NULL_ESTABLISH.confirm	MAC_ESTABLISH.confirm
CL_NULL_RELEASE.request	MAC_RELEASE.request
CL_NULL_RELEASE.indication	MAC_RELEASE.indication
CL_NULL_RELEASE.response	MAC_RELEASE.response
CL_NULL_RELEASE.confirm	MAC_RELEASE.confirm
CL_NULL_JOIN.request	MAC_JOIN.request
CL_NULL_JOIN.indication	MAC_JOIN.indication
CL_NULL_JOIN.response	MAC_JOIN.response
CL_NULL_JOIN.confirm	MAC_JOIN.confirm
CL_NULL_LEAVE.request	MAC_LEAVE.request
CL_NULL_LEAVE.indication	MAC_LEAVE.indication
CL_NULL_LEAVE.response	MAC_LEAVE.response
CL_NULL_LEAVE.confirm	MAC_LEAVE.confirm
CL_NULL_DATA.request	MAC_DATA.request
CL_NULL_DATA.indication	MAC_DATA.indication
CL_NULL_DATA.confirm	MAC_DATA.confirm
CL_NULL_SEND.request	MAC_SEND.request
CL_NULL_SEND.indication	MAC_SEND.indication
CL_NULL_SEND.confirm	MAC_SEND.confirm

2915

2916 5.4 IPv4 Podwarstwa konwergencji właściwa dla usługi (SSCS IPv4)

2917 5.4.1 Omówienie

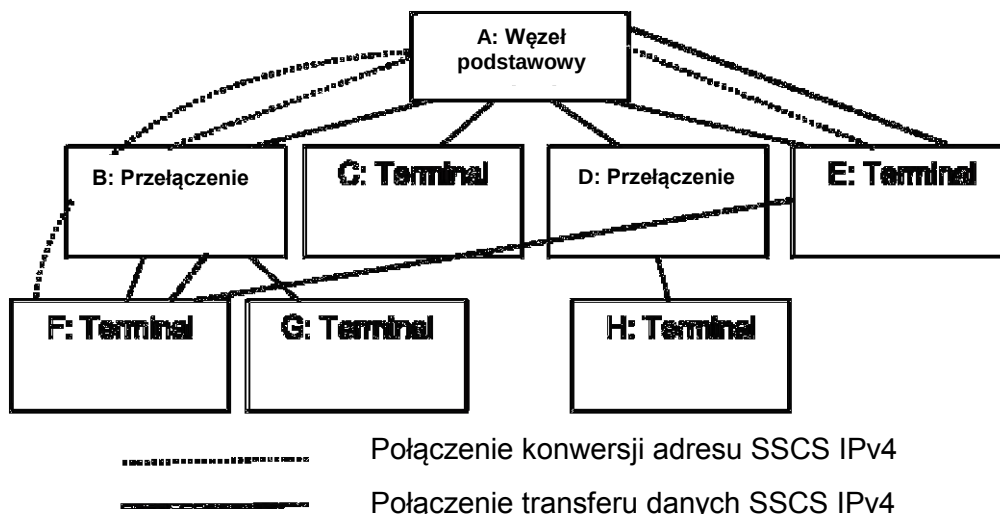
2918 Podwarstwa SSCS IPv4 zapewnia skuteczną metodę przesyłania pakietów IPv4 przez podsieci OFDM PRIME.
 2919 Zastosowanie ma kilka konwencji:

- 2920 • Węzeł serwisowy może wysyłać pakiety IPv4 tylko do węzła podstawowego lub innych węzłów
 2921 serwisowych.
- 2922 • Zakłada się, że węzeł podstawowy działa jak router pomiędzy podsiecią OFDM PRIME i inną siecią.
 2923 Węzeł podstawowy może również działać jako NAT. W jaki sposób węzeł podstawowy łączy się z
 2924 innymi sieciami wykracza poza zakres niniejszej specyfikacji.
- 2925 • W celu uproszczenia wdrożeń, jeden lokalny adres IPv4 obsługuje tylko jedną ścieżkę.
- 2926 • Węzły serwisowe muszą korzystać ze statycznie skonfigurowanych adresów IPv4 lub DHCP, aby
 2927 uzyskać adresy IPv4.
- 2928 • Węzeł podstawowy przeprowadza konwersję adresu IPv4 do EUI-48. Każdy węzeł serwisowy
 2929 rejestruje swój adres IPv4 i adres EUI-48 w węźle podstawowym (patrz punkt 5.4.2). Inne węzły
 2930 serwisowe mogą następnie wysyłać zapytania do węzła podstawowego w celu konwersji adresu IPv4

na adres EUI-48. Wymaga to ustanowienia dedykowanego połączenia z węzłem podstawowym celem konwersji adresu.

- SSCS IPv4 wykonuje routing pakietów IPv4. Innymi słowy podwarstwa SSCS IPv4 zdecyduje czy pakiet powinien być wysłany bezpośrednio do innego węzła serwisowego lub przesłany do konfigurowanej bramy.
- Mimo że IPv4 jest protokołem bezpołączeniowym, warstwa konwergencji IPv4 jest zorientowana na połączenie. Gdy konwersja adresu została już przeprowadzona, połączenie ustanowiono pomiędzy węzłem serwisowym źródłowym a węzłem docelowym do przesyłania pakietów IPv4. Połączenie to utrzymywane jest podczas transferu ruchu i może zostać zamknięte po okresie braku aktywności.
- SAR podwarstwy CPCS (patrz punkt 5.2) powinien być zawsze obecny w warstwie konwergencji IPv4. Wygenerowane MSDU mają co najwyżej długość CIMTUSize bajtów, a komunikaty PDU górnej warstwy nie mogą być dłuższe niż CIMaxAppPktSize.
- Opcjonalnie nagłówki TCP/IPv4 można kompresować. Kompresja jest negocjowana jako część fazy ustanawiania połączenia.
- Transmisja pakietów IPv4 jest obsługiwana za pomocą mechanizmu transmisji broadcast MAC.
- Multicasting pakietów IPv4 jest obsługiwany za pomocą mechanizmu transmisji multicast MAC.

SSCS IPv4 posiada kilka typów połączeń. Dla konwersji adresu istnieje połączenie do węzła podstawowego. W przypadku transferu danych IPv4, na węzeł docelowy występuje jedno połączenie: z węzłem podstawowym, który działa jako bramka IPv4 do innych sieci lub do/z innym węzłem w tej samej podsieci. Pokazano to na Rys. 98.



Rys. 98 - Przykład połączenia podwarstwy SSCS IPv4

W tym miejscu węzły B, E i F połączone są połączeniami konwersji adresu do węzła podstawowego. Węzeł E ma ustanowione połączenie danych z węzłem podstawowym i węzłem F. Węzeł F również połączony jest połączeniem danych z węzłem B. Rysunek nie pokazuje połączeń broadcast i multicast.

2956 **5.4.2 Konwersja adresu**

2957 **5.4.2.1 Ogólne**

2958 Warstwa IPv4 dostarczy podwarstwie SSCS IPv4 pakiet IPv4 do przesłania. Podwarstwa SSCS IPv4
2959 odpowiada za określenie, do którego węzła serwisowego dostarczony powinien zostać pakiet za pomocą
2960 adresów IPv4 w tym pakiecie. Podwarstwa SSCS IPv4 musi następnie ustanowić połączenie z węzłem
2961 docelowym jeśli takie jeszcze nie istnieje, tak aby pakiet można było przesłać. Stosować można trzy klasy
2962 adresów IPv4, a następne podpunkty opisują sposób konwersji tych adresów na adresy EUI-48.

2963 **5.4.2.2 Adresy Unicast**

2964 **5.4.2.2.1 Ogólne**

2965 Adresy unicast IPv4 muszą zostać przekonwertowane na adresy unicast EUI-48. Węzeł podstawowy
2966 zarządza bazą danych adresów IPv4 i adresów EUI-48. Konwersja adresu następnie działa poprzez wysłanie
2967 do tej bazy danych zapytań. Węzeł podstawowy musi ustanowić połączenie z usługą konwersji adresów
2968 pracującą na węźle podstawowym za pomocą wartości typu połączenia TYPE (patrz Załącznik E)
2969 TYPE_CL_IPv4_AR. Żadne dane nie powinny być przekazywane w nawiązaniu połączenia. Za pomocą tego
2970 połączenia węzeł serwisowy może skorzystać z dwóch mechanizmów określonych w kolejnych akapitach.

2971 **5.4.2.2.2 Rejestrowanie i wyrejestrowywanie adresu**

2972 Węzeł serwisowy stosuje komunikat AR_REGISTER_S do zarejestrowania adresu IPv4 i odpowiadającego mu
2973 adresu EUI-48 oznaczającego żądanie z węzła podstawowego do zarejestrowania adresu IPv4 i
2974 odpowiedniego EUI-48 węzła serwisowego w tablicy rejestracji. Węzeł podstawowy zatwierdzi komunikat
2975 AR_REGISTER_B. Węzeł serwisowy może rejestrować wiele adresów IPv4 dla tego samego adresu EUI-48.

2976 Węzeł serwisowy stosuje komunikat AR_DEREGISTER_S do wyrejestrowania adresu IPv4 i odpowiadającego
2977 mu adresu EUI-48 oznaczającego żądanie z węzła podstawowego do usunięcia wpisów odpowiadających
2978 danemu adresowi IPv4 z tablicy rejestracji. Węzeł podstawowy zatwierdzi go komunikatem
2979 AR_REGISTER_B.

2980 Gdy połączenie konwersji adresu IPv4 pomiędzy węzłem serwisowym, a węzłem podstawowym zostanie
2981 zamknięte, węzeł podstawowy usunie wszystkie adresy powiązane z tym połączeniem.

2982 **5.4.2.2.3 Wyszukiwanie adresu**

2983 Węzeł serwisowy korzysta z komunikatu AR_LOOKUP_S do przeprowadzania wyszukiwania. Komunikat
2984 zawiera adres IPv4 do konwersji. Węzeł podstawowy odpowie za pomocą komunikatu AR_LOOKUP_B, który
2985 zawiera kod błędu i, jeśli nie ma żadnych błędów, adres EUI-48 powiązany z adresem IPv4. Jeśli węzeł
2986 podstawowy ma wiele wpisów w swojej bazie danych dla tego samego adresu IPv4, możliwy zwrócony
2987 adres EUI-48 nie jest zdefiniowany.

2988 **5.4.2.3 Adres Broadcast**

2989 Adres broadcast IPv4 255.255.255.255 mapuje się na połączenie MAC broadcast z LCID równym
2990 LCI_CL_IPv4_BROADCAST. Wszystkie pakiety broadcast IPv4 zostaną wysłane do tego połączenia. Gdy w
2991 tym połączeniu zostanie odebrany pakiet broadcast IPv4, adres IPv4 należy sprawdzić, celem stwierdzenia

czy jest to pakiet broadcast dla podsieci, w której węzeł posiada adres IPv4. Do stosu protokołu IPv4 wysyłane powinny być jedynie pakiety broadcast z podsieci członkowskich.

5.4.2.4 Adresy multicast

Adresy multicast IPv4 mapowane są na połączenie multicast OFDM PRIME MAC przez węzeł podstawowy za pomocą protokołu konwersji adresu.

Aby dołączyć do grupy multicast, z węzła serwisowego do węzła podstawowego za pomocą adresu multicast wysyłany jest atrybut AR_MCAST_REG_S. Węzeł podstawowy odpowie za pomocą AR_MCAST_REG_B zawierającego wartość LCID przydzieloną do określonego adresu multicast. Jednakże węzeł podstawowy, według uznania, może również przypisać inne identyfikatory LCID, które nie są używane. Węzeł serwisowy może następnie dołączyć do grupy multicast (patrz 4.6.7.2) dla danego LCID, aby odbierać pakiety multicast IPv4. Te wartości LCID mogą być ponownie używane, tak aby wiele adresów docelowych multicast IPv4 można było zobaczyć w tym samym LCID. Aby opuścić grupę multicast, z węzła serwisowego do węzła podstawowego za pomocą adresu multicast IPv4 wysyłany jest atrybut AR_MCAST_UNREG_S. Węzeł podstawowy zatwierdzi go komunikatem AR_MCAST_UNREG_B.

Gdy węzeł serwisowy chce wysłać datagram multicast IPv4, po prostu używa odpowiedniego LCID. Jeśli węzeł serwisowy nie dołączył do grupy multicast, musi najpierw nauczyć się LCID, który ma być używany. Można wykorzystać proces z komunikatami AR_MCAST_REG_{S|B} jak opisano wyżej. Podczas, gdy pakiety multicast IPv4 są stale wysyłane, węzeł serwisowy pozostaje zarejestrowany w grupie multicast. T_{mcast_reg} po wysłaniu ostatniego datagramu multicast IPv4 węzeł serwisowy powinien wyrejestrować się z grupy multicast za pomocą komunikatów AR_MCAST_UNREG_{S|B}. Wartość nominalna T_{mcast_reg} to 10 minut, jednakże stosować można inne wartości.

5.4.2.5 Retransmisja pakietów konwersji adresu

Połączenie pomiędzy węzłem serwisowym a węzłem podstawowym dla konwersji adresu nie jest niezawodne jeśli nie stosuje się MAC ARQ. Węzeł serwisowy do retransmisji jeśli węzeł podstawowy nie odpowiada w ciągu jednej sekundy. Nie jest błędem, gdy węzeł podstawowy otrzymuje te same żądania rejestracji kilka razy lub jest proszony o usunięcie rejestracji, która nie istnieje. Warunki te mogą być wynikiem retransmisji.

5.4.3 Transfer pakietu IPv4

Dla pakietów do przeniesienia należy ustanowić połączenie pomiędzy węzłem źródłowym a docelowym. Podwarstwa SSCS IPv4 sprawdzi każdy pakiet, aby określić docelowy adres EUI-48. Jeśli połączenie danych z punktem docelowym zostało już ustanowione, pakiet jest wysyłany. Aby tego dokonać, SSCS IPv4 zarządza tabelą dla każdego połączenia zawierającą informacje podane w Tabeli 55 (patrz RFC 1144). Aby skorzystać z tej tabeli, konieczne jest określenie czy adres docelowy IPv4 znajduje się w lokalnej podsieci lub czy należy użyć bramki. W tym celu stosowana jest maska podsieci skojarzona z lokalnym adresem IPv4. Jeśli adres docelowy IPv4 nie znajduje się w lokalnej podsieci, podczas przeszukiwania tabeli zamiast adresu docelowego stosowany jest adres bramy domyślnej.

Tabela 55 - Pozycja tablicy SSCS IPv4

Parametr	Opis
CL_IPv4_Con.Remote_IP	Zdalny adres IPv4 tego połączenia.
CL_IPv4_Con.ConHandle	Uchwyt połączenia MAC dla połączenia.
CL_IPv4_Con.LastUsed	Data i czas ostatniego odebranego/wysłanego pakietu.
CL_IPv4_Con.HC	Stosowany schemat kompresji nagłówka.
CL_IPv4_CON.RxSeq	Następna oczekiwana liczba sekwencji odbierania.
CL_IPv4_CON.TxSeq	Liczba sekwencji kolejnej transmisji.

3029 Podwarstwa SSCS IPv4 może zamknąć połączenie, gdy nie zostało ono wykorzystane do określonego przez
 3030 realizację okresu czasu. Kiedy połączenie jest zamykane, wejście do podłączenia jest usuwane na obu
 3031 końcach połączenia.

3032 Gdy połączenie do miejsca przeznaczenia nie istnieje, konieczne są dodatkowe prace. Usługa konwersji
 3033 adresu stosowana jest do określenia adresu EUI-48 zdalnego adresu IPv4 jeśli jest on adresem lokalnym lub
 3034 bramy skojarzonej z lokalnym adresem jeśli adres docelowy znajduje się w kolejnej podsieci. Jeśli węzeł
 3035 podstawowy odpowiada za pomocą adresu EUI-48 docelowego węzła serwisowego, ustanawiane jest
 3036 połączenie MAC ze zdalnym urządzeniem. Wartość TYPE tego połączenia to TYPE_CL_IPv4_UNICAST. Dane
 3037 przekazywane w komunikacie żądania określono w punkcie 5.4.7.4. Lokalny adres IPv4 jest podawany po to,
 3038 aby zdalne urządzenie mogło dodać nowe połączenie do pamięci podręcznej połączeń do przesyłania
 3039 danych w przeciwnym kierunku. Korzystanie z kompresji nagłówków Van Jacobsona jest również
 3040 wynegocjowana w ramach ustanawiania połączenia. Po nawiązaniu połączenia, pakiety IPv4 mogą być
 3041 wysyłane.

3042 Gdy pakiet jest skierowany do adresu broadcast IPv4, pakiet musi zostać wysłany za pomocą usługi
 3043 broadcast MAC. Gdy otwarta jest podwarstwa SSCS IPv4, nawiązywane jest połączenie broadcast do
 3044 przesyłania wszystkich pakietów broadcast. Pakiet broadcast IPv4 jest po prostu wysyłany do tego
 3045 połączenia. Każdy pakiet odbierany na tym połączeniu broadcast jest przekazywany do stosu protokołu
 3046 IPv4.

3047 **5.4.4 Podział i scalanie**

3048 Podwarstwa SSCS IPv4 powinna obsługiwać pakiety IPv4 przy MTU wynoszącej 1500 bajtów. Wymaga to
 3049 zastosowania podziału i scalania SAR (patrz 5.2.2).

3050 **5.4.5 Kompresja nagłówka**

3051 Kompresja nagłówków TCP/IP Van Jacobsona to funkcja opcjonalna w podwarstwie SSCS IPv4. Użycie
 3052 kompresji VJ jest negocjowane jako część fazy ustanawiania połączenia pomiędzy dwoma węzłami
 3053 serwisowymi.

3054 Kompresja VJ jest przeznaczona do stosowania w warstwie łącza punkt-punkt, które może informować
 3055 dekompresor, gdy pakiety zostały uszkodzone lub utracone. Podczas wystąpienia błędów lub utraty

3056 pakietów dekompresor może ponownie zsynchronizować się z kompresorem. Bez tego proces
3057 resynchronizacji generowane będą błędne pakiety i przekazywane do stosu IPv4.

3058 Warstwa MAC nie oferuje obiektu do wykrywania utraty pakietów lub zgłaszania uszkodzonych pakietów.
3059 Tym samym konieczne jest dodanie tej funkcjonalności do podwarstwy SSCS IPv4. Podwarstwa SSCS
3060 utrzymuje dwie kolejne liczby sekwencji gdy dla połączenia włączona jest kompresja VJ. Te liczby sekwencji
3061 mają wielkość 8 bitów. Podczas przesyłania pakietu IPv4, liczba sekwencji CL_IPv4_CON.TxSeq umieszczana
3062 jest w nagłówku pakietu jak pokazano w punkcie 5.4.3. Liczba sekwencji następnie się zwiększa. Po
3063 otrzymaniu pakietu, liczba sekwencji w odebranym pakiecie jest porównywana z CL_IPv4_CON.RxSeq. Jeśli
3064 liczby te różnią się, do dekompresora przekazywany jest parametr TYPE_ERROR, zgodnie z RFC1144.
3065 Wartość CL_IPv4_CON.RxSeq jest zawsze aktualizowana do wartości odbieranej w nagłówku pakietu.

3066 Kompresja nagłówka nigdy nie powinna być negocjowana dla pakietów broadcast lub multicast.

3067 5.4.6 Mapowanie jakości usług

3068 MAC PRIME OFDM określa czy mechanizm współdzielonej kontencji obsługuje 4 poziomy pierwszeństwa (1-
3069 4). Poziom 1 stosowany jest dla wiadomości sygnalizacyjnych MAC, ale nie tylko.

3070 Pakiety IPv4 zawierają w nagłówku pole Typu usługi w celu wskazania jakości usługi, jaką pakiet chciałby
3071 otrzymać. Trzy bity TOS wskazują pierwszeństwo IP. Poniższa tabela określa sposób mapowania
3072 pierwszeństwa IP na priorytet MAC OFDM PRIME.

3073 Tabela 56 - Mapowanie pierwszeństwa IPv4 na priorytet MAC OFDM PRIME

Pierwszeństwo IP	Priorytet MAC
000 – Ruch zwyczajny	4
001 – Ruch nadrzędny	4
010 – Ruch natychmiastowy	3
011 – Ruch błyskawiczny	3
100 – Ruch ponadbłyskawiczny	2
101 – Ruch krytyczny	2
110 – Ruch kontroli intersieci WAN	1
111 – Ruch kontroli sieci	1

3074

3075 **Uwaga:** Na poziomie warstwy MAC priorytet podany w polu nagłówka pakietu jest wartością przypisywaną
3076 w tej tabeli minus 1, ponieważ zakres pola PKT.PRIO wynosi od 0 do 3.

3077 5.4.7 Formaty pakietów i dane połączenia

3078 5.4.7.1 Ogólne

3079 Punkt ten określa format jednostek PDU podwarstwy SSCS IPv4.

3080 5.4.7.2 Jednostki PDU konwersji adresu

3081 5.4.7.2.1 Ogólne

3082 Kolejne PDU są przesyłane za pomocą połączenia konwersji adresu pomiędzy węzłem serwisowym, a
 3083 węzłem podstawowym. Poniższe punkty określają wartości AR.MSG w zakresie od 0 do 11. Wszystkie
 3084 wyższe wartości są zarezerwowane dla nowszych wersji tej specyfikacji.

3085 5.4.7.2.2 AR_REGISTER_S

3086 Tabela 57 pokazuje komunikat rejestracji konwersji adresu wysłany z węzła serwisowego do węzła
 3087 podstawowego.

3088 Tabela 57 - Format komunikatu AR_REGISTER_S

Nazwa	Długość	Opis
AR.MSG	8 bitów	Typ komunikatu konwersji adresu. • Dla AR_REGISTER_S = 0.
AR.IPv4	32 bity	Adres IPv6 do zarejestrowania.
AR.EUI-48	48 bitów	EUI-48 do zarejestrowania.

3089 5.4.7.2.3 AR_REGISTER_B

3090 Tabela 58 pokazuje komunikat zatwierdzenia rejestracji konwersji adresu wysłany z węzła podstawowego
 3091 do węzła serwisowego.

3092 Tabela 58 - Format komunikatu AR_REGISTER_B

Nazwa	Długość	Opis
AR.MSG	8 bitów	Typ komunikatu konwersji adresu. • Dla AR_REGISTER_B = 1.
AR.IPv4	32 bity	Zarejestrowany adres IPv4.
AR.EUI-48	48 bitów	EUI-48 zarejestrowany.

3093

3094 Pola AR.IPv4 i AR.EUI-48 są ujęte w komunikacie AR_REGISTER_B, więc węzeł serwisowy może
3095 przeprowadzać wiele nakładających się na siebie rejestracji.

3096 5.4.7.2.4 AR_UNREGISTER_S

3097 Tabela 59 pokazuje komunikat wyrejestrowania konwersji adresu wysłany z węzła serwisowego do węzła
3098 podstawowego.

3099 Tabela 59 - format komunikatu AR_UNREGISTER_S

Nazwa	Długość	Opis
AR.MSG	8 bitów	Typ komunikatu konwersji adresu. Dla AR_UNREGISTER_S = 2.
AR.IPv4	32 bity	Adres IPv4 do wyrejestrowania.
AR.EUI-48	48 bitów	EUI-48 do wyrejestrowania.

3100 5.4.7.2.5 AR_UNREGISTER_B

3101 Tabela 60 pokazuje komunikat zatwierdzenia wyrejestrowania konwersji adresu wysłany z węzła
3102 podstawowego do węzła serwisowego.

3103 Tabela 60 - format komunikatu AR_UNREGISTER_B

Nazwa	Długość	Opis
AR.MSG	8 bitów	Typ komunikatu konwersji adresu. Dla AR_UNREGISTER_B = 3.
AR.IPv4	32 bity	Wyrejestrowany adres IPv4.
AR.EUI-48	48 bitów	Wyrejestrowany EUI-48.

3104 Pola AR.IPv4 i AR.EUI-48 są ujęte w komunikacie AR_UNREGISTER_B, więc węzeł serwisowy może
3105 przeprowadzać wiele nakładających się na siebie wyrejestrowań.

3106 5.4.7.2.6 AR_LOOKUP_S

3107 Tabela 61 pokazuje komunikat wyszukiwania konwersji adresu wysłany z węzła serwisowego do węzła
3108 podstawowego.

3109 Tabela 61 - format komunikatu AR_LOOKUP_S

Nazwa	Długość	Opis
AR.MSG	8 bitów	Typ komunikatu konwersji adresu.

		Dla AR_LOOKUP_S = 4.
AR.IPv4	32 bity	Adres IPv4 do wyszukania.

3110 5.4.7.2.7 AR_LOOKUP_B

3111 Tabela 62 pokazuje komunikat wyszukiwania konwersji adresu wysłany z węzła podstawowego do węzła
3112 serwisowego.

3113 Tabela 62 - format komunikatu AR_LOOKUP_B

Nazwa	Długość	Opis
AR.MSG	8 bitów	Typ komunikatu konwersji adresu. Dla AR_LOOKUP_B = 5.
AR.IPv4	32 bity	Wyszukany adres IPv4.
AR.EUI-48	48 bitów	EUI-48 dla adresu IPv4.
AR.Status	8 bitów	Status wyszukiwania wskazujący czy adres został znaleziony, czy też wystąpił błąd. 0 = znaleziony, AR.EUI-48 prawidłowy; 1 = nieznany, AR.EUI-48 niezdefiniowany.

3114 Wyszukiwanie może nie powieść się, jeśli żądany adres nie został zarejestrowany. W tym przypadku
3115 AR.Status będzie miał wartość inną niż zero, a treść AR.EUI-48 będzie niezdefiniowana. Wyszukiwanie jest
3116 skuteczne jedynie, gdy AR.Status wynosi zero. W tym przypadku EUI-48 zawiera przekonwertowany adres.

3117 5.4.7.2.8 AR_MCAST_REG_S

3118 Tabela 63 pokazuje komunikat rejestracji konwersji adresu multicast wysłany z węzła serwisowego do węzła
3119 podstawowego.

3120 Tabela 63 - format komunikatu AR_MCAST_REG_S

Nazwa	Długość	Opis
AR.MSG	8 bitów	Typ komunikatu konwersji adresu. Dla AR_MCAST_REG_S = 8.
AR.IPv4	32 bity	Adres multicast IPv4 do zarejestrowania.

3121 5.4.7.2.9 AR_MCAST_REG_B

3122 Tabela 64 pokazuje komunikat rejestracji konwersji adresu multicast wysłany z węzła podstawowego do
3123 węzła serwisowego.

3124 Tabela 64 - format komunikatu AR_MCAST_REG_B

Nazwa	Długość	Opis
AR.MSG	8 bitów	Typ komunikatu konwersji adresu. Dla AR_MCAST_REG_B = 9.
AR.IPv4	32 bity	Zarejestrowany adres multicast IPv4.
<i>Reserved</i>	2 bity	Zarezerwowany. Powinien być kodowany jako 0.
AR.LCID	6 bitów	Identyfikator połączenia lokalnego przypisany do tego adresu IPv4 multicast.

3125

3126 Pole AR.IPv4 jest ujęte w komunikacie AR_MCAST_REG_B, więc węzeł serwisowy może przeprowadzać
3127 wiele nakładających się na siebie rejestracji.

3128 5.4.7.2.10 AR_MCAST_UNREG_S

3129 Tabela 65 pokazuje komunikat wyrejestrowania konwersji adresu multicast wysłany z węzła serwisowego
3130 do węzła podstawowego.

3131 Tabela 65 - format komunikatu AR_MCAST_UNREG_S

Nazwa	Długość	Opis
AR.MSG	8 bitów	Typ komunikatu konwersji adresu. Dla AR_MCAST_UNREG_S = 10.
AR.IPv4	32 bity	Adres multicast IPv4 do wyrejestrowania.

3132 5.4.7.2.11 AR_MCAST_UNREG_B

3133 Tabela 66 pokazuje komunikat wyrejestrowania konwersji adresu multicast wysłany z węzła podstawowego
3134 do węzła serwisowego.

3135 Tabela 66 - format komunikatu AR_MCAST_UNREG_B

Nazwa	Długość	Opis
AR.MSG	8 bitów	Typ komunikatu konwersji adresu. Dla AR_MCAST_UNREG_B = 11;
AR.IPv4	32 bity	Wyrejestrowany adres multicast IPv4.

3136

3137 Pole AR.IPv4 jest ujęte w komunikacie AR_MCAST_UNREG_B, więc węzeł serwisowy może przeprowadzać
3138 wiele nakładających się na siebie wyrejestrowań.

3139 5.4.7.3 Format pakietu IPv4

3140 5.4.7.3.1 Ogólne

3141 Następujące formaty PDU stosowane są do przesyłania pakietów IPv4 pomiędzy węzłami serwisowymi.
 3142 Zdefiniowano dwa formaty. Pierwszy format używany jest wtedy, gdy nie jest stosowana kompresja
 3143 nagłówka. Drugi format jest dla kompresji nagłówka Van Jacobsona.

3144 5.4.7.3.2 Format pakietu IPv4, Brak wynegocjowanej kompresji nagłówka

3145 Jeśli nie wynegocjowano kompresji nagłówka, pakiet IPv4 wysyłany jest w takim stanie, bez nagłówka.

3146 Tabela 67 - Format pakietu IPv4 bez wynegocjowanej kompresji nagłówków

Nazwa	Długość	Opis
<i>IPv4.PKT</i>	n- oktetów	Pakiet IPv4.

3147 5.4.7.3.3 Format pakietu IPv4 z kompresją nagłówków VJ

3148 Przy kompresji nagłówka Van Jacobsona przed pakietem IPv4 niezbędny jest nagłówek jednooktetowy.

3149 Tabela 68 - Format pakietu IPv4 z wynegocjowaną kompresją nagłówków

Nazwa	Długość	Opis
IPv4.Type	2 bity	Typ skompresowanego pakietu. • IPv4.Type = 0 – TYPE_IP; • IPv4.Type = 1 – UNCOMPRESSED_TCP; • IPv4.Type = 2 – COMPRESSED_TCP; • IPv4.Type = 3 – TYPE_ERROR.
IPv4.Seq	6 bitów	Liczba sekwencji pakietu.
<i>IPv4.PKT</i>	n- oktetów	Pakiet IPv4.

3150

3151 Wartość typu IPv4 TYPE_ERROR nigdy nie jest wysyłana. Jest to pseudo pakiet stosowany do
 3152 powiadomienia dekompresora, że pakiet został utracony.

3153 5.4.7.4 Dane połączenia

3154 5.4.7.4.1 Ogólne

3155 Gdy pomiędzy węzłami serwisowymi nawiązano połączenie do przesyłania pakietów IPv4, dane przesyłane
 3156 są również w pakietach żądania połączenia. Dane te pozwalają na negocjacje kompresji i powiadomienie
 3157 adresu IPv4.

3158 5.4.7.4.2 Dane połączenia od inicjatora

3159 Tabela 69 pokazuje dane połączenia wysyłane przez inicjatora.

3160 Tabela 69 - Dane sygnalizacji połączenia wysyłane przez inicjatora

Nazwa	Długość	Opis
<i>Reserved</i>	6 bitów	Powinien być kodowany jako 0 dla tej wersji protokołu SSCS IPv4.
Data.HC	2 bity	Kompresja nagłówka. - Data.HC = 0 – Brak żądania kompresji; - Data.HC = 1 – Żądanie kompresji VJ; - Data.HC = 2, 3 – Zarezerwowany dla przyszłych wersji specyfikacji.
Data.IPv4	32 bity	Adres IPv4 inicjatora.

3161 Jeśli urządzenie przyjmuje połączenie, powinno one skopiować adres Data.IPv4 do nowej pozycji tablicy
3162 wraz z wynegocjowaną wartością Data.HC.

3163 5.4.7.4.3 Dane połączenia od respondenta

3164 Tabela 70 70 pokazuje dane połączenia wysyłane w odpowiedzi na żądanie połączenia.

3165 Tabela 70 70 - Dane sygnalizacji połączenia wysyłane przez respondenta

Nazwa	Długość	Opis
<i>Reserved</i>	6 bitów	Powinien być kodowany jako 0 dla tej wersji protokołu SSCS IPv4.
Data.HC	2 bity	Wynegocjowana kompresja nagłówka. - Data.HC = 0 – Kompresja niedozwolona; - Data.HC = 1 – Wynegocjowano kompresję VJ; - Data.HC = 2,3 – Zarezerwowany.

3166

3167 Schemat kompresji nagłówka może być zastosowany wyłącznie, jeśli obsługiwany jest przez węzły
3168 serwisowe. Respondent może jedynie ustawić Data.HC na 0 lub na tę samą wartość, jak wartość odebrana
3169 od inicjatora. Gdy stosowana jest ta sama wartość, wskazuje ona, że żądany schemat kompresji został
3170 wynegocjowany i będzie stosowany dla tego połączenia. Ustawienie Data.HC na 0 pozwala respondentowi
3171 na odmówienie żądania dla tego schematu kompresji nagłówka lub wymuszenie nieużywania kompresji
3172 nagłówka.

3173 5.4.8 Punkt dostępu do usługi

3174 5.4.8.1 Ogólne

3175 Ten punkt określa punkt dostępu do usług stosowany przez warstwę IPv4 do komunikowania się z SSCS
3176 IPv4.

5.4.8.2 Obsługa i zamykanie SSCS IPv4**5.4.8.2.1 Ogólne**

Poniższe prymitywy stosowane są do otwierania i zamykania SSCS IPv4. Podwarstwa SSCS IPv4 może być otwarta tylko raz. Warstwa IPv4 może zamknąć SSCS IPv4, gdy interfejs IPv4 zostanie zamknięty. IPv4 również zamknie SSCS IPv4, gdy podstawowe połączenie MAC do węzła podstawowego zostało utracone.

5.4.8.2.2 CL_IPv4_ESTABLISH.request

Prymityw CL_IPv4_ESTABLISH.request przekazywany jest z warstwy IPv4 do warstwy SSCS IPv4. Stosowany jest, gdy warstwa IPv4 przenosi interfejs w górę.

Semantyka tego prymitywu przedstawia się następująco:

CL_IPv4_ESTABLISH.request{}

Po odebraniu tego prymitywu SSCS IPv4 utworzy połączenie konwersji adresu do węzła podstawowego i dołączy do grupy broadcast stosowanej do odbierania/przesyłania pakietów broadcast.

5.4.8.2.3 CL_IPv4_ESTABLISH.confirm

Prymityw CL_IPv4_ESTABLISH.confirm przekazywany jest z podwarstwy SSCS IPv4 do warstwy IPv4. Stosowany jest do wskazania, czy podwarstwa SSCS IPv4 jest gotowa do uzyskania dostępu do pakietów IPv4 przesyłanych do warstw równorzędnych.

Semantyka tego prymitywu przedstawia się następująco:

CL_IPv4_ESTABLISH.confirm{}

Gdy podwarstwa SSCS IPv4 ustanowi wszystkie niezbędne połączenia i jest gotowa na przesłanie i odbieranie pakietów IPv4, prymityw ten przekazywany jest do warstwy IPv4. Jeśli podwarstwa SSCS IPv4 napotka na błąd podczas otwierania, odpowie za pomocą prymitywu CL_IPv4_RELEASE, a nie prymitywu CL_IPv4_ESTABLISH.confirm.

5.4.8.2.4 CL_IPv4_RELEASE.request

Prymityw CL_IPv4_RELEASE.request stosowany jest przez warstwę IPv4, gdy interfejs jest zamknięty. SSCS IPv4 zamyka wszystkie połączenia tak, aby żadne inne pakiety nie były otrzymywane, a wszystkie inne zasoby zostały zwolnione.

Semantyka tego prymitywu przedstawia się następująco:

CL_IPv4_RELEASE.request{}

Gdy SSCS IPv4 zwolni wszystkie swoje połączenia i zasoby, zwróci prymityw CL_IPv4_RELEASE.confirm.

5.4.8.2.5 CL_IPv4_RELEASE.confirm

Prymityw CL_IPv4_RELEASE.confirm stosowany jest przez SSCS IPv4 do wskazywania warstwie IPv4, że podwarstwa SSCS IPv4 została zamknięta. Może nastąpić to w wyniku prymitywu CL_IPv4_RELEASE.request

3209 prymitywu `CL_IPv4_ESTABLISH.request` lub ponieważ warstwa MAC wskazuje, że połączenie konwersji
3210 adresu zostało utracone lub sam węzeł serwisowy nie jest już zarejestrowany.

3211 Semantyka tego prymitywu przedstawia się następująco:

3212 `CL_IPv4_RELEASE.confirm{result}`

3213 Parametr *Result* ma znaczenie określone w Tabeli 134.

3214 **5.4.8.3 Zarządzanie adresem Unicast**

3215 **5.4.8.3.1 Ogólne**

3216 Opisane tu prymitywy są stosowane do zarządzania adresami, tj. rejestracji i wyrejestrowywania adresów
3217 powiązanych z tą SSCS IPv4.

3218 W przypadku braku adresów IPv4 skojarzonych z SSCS IPv4, podwarstwa SSCS IPv4 jedynie wysyła i odbiera
3219 pakiety broadcast i multicast. Pakietów unicast nie można wysłać. Jednakże jest to wystarczające dla
3220 działania BOOTP/DHCP, aby pozwolić urządzeniu na uzyskanie adresu IPv4. Po zarejestrowaniu adresu IPv4
3221 warstwa IPv4 może przysyłać pakiety unicast, które mają adres źródłowy równy jednemu z jej
3222 zarejestrowanych adresów.

3223 **5.4.8.3.2 CL_IPv4_REGISTER.request**

3224 Ten prymityw przekazywany jest z warstwy IPv4 do SSCS IPv4 w celu zarejestrowania adresu IPv4.

3225 Semantyka tego prymitywu przedstawia się następująco:

3226 `CL_IPv4_REGISTER.request{IPv4, netmask, gateway}`

3227 Adres IPv4 to adres do zarejestrowania.

3228 Maska sieciowa jest maską sieci wykorzystaną do maskowania numeru sieci z adresu. Maski podsieci
3229 używana jest przez podwarstwę SSCS IPv4 do określenia czy pakiet powinien być dostarczany bezpośrednio
3230 lub czy należy zastosować bramę.

3231 Brama jest adresem IPv4 stosowanym dla pakietów z lokalnym adresem IPv4, ale z adresem docelowym
3232 innym niż adres lokalny podsieci.

3233 Gdy adres IPv4 został zarejestrowany w węźle podstawowym, stosowany jest prymityw `CL_IPv4_REGISTER`.
3234 Jeśli rejestracja zakończy się niepowodzeniem, zastosowany zostanie prymityw `CL_IPv4_RELEASE.confirm`.

3235 **5.4.8.3.3 CL_IPv4_REGISTER.confirm**

3236 Ten prymityw przekazywany jest z podwarstwy SSCS IPv4 do warstwy IPv4 w celu wskazania, że rejestracja
3237 zakończyła się powodzeniem.

3238 Semantyka tego prymitywu przedstawia się następująco:

3239 `CL_IPv4_REGISTER.confirm{IPv4}`

3240 Adres IPv4 to adres, który został zarejestrowany.

3241 Po zakończeniu rejestracji warstwa IPv4 może wysyłać pakiety IPv4 za pomocą adresu źródłowego.

3242 **5.4.8.3.4 CL_IPv4_UNREGISTER.request**

3243 Ten prymityw przekazywany jest z warstwy IPv4 do SSCS IPv4 w celu wyrejestrowania adresu IPv4.

3244 Semantyka tego prymitywu przedstawia się następująco:

3245 *CL_IPv4_UNREGISTER.request{IPv4}*

3246 Adres IPv4 to adres do wyrejestrowania.

3247 Gdy adres IPv4 został wyrejestrowany z węzła podstawowego, stosowany jest prymityw
3248 CL_IPv4_UNREGISTER. Jeśli wyrejestrowanie zakończy się niepowodzeniem, zastosowany zostanie
3249 prymityw CL_IPv4_RELEASE.confirm.

3250 **5.4.8.3.5 CL_IPv4_UNREGISTER.confirm**

3251 Ten prymityw przekazywany jest z podwarstwy SSCS IPv4 do warstwy IPv4 w celu wskazania, że
3252 wyrejestrowanie zakończyła się powodzeniem.

3253 Semantyka tego prymitywu przedstawia się następująco:

3254 *CL_IPv4_UNREGISTER.confirm{IPv4}*

3255 Adres IPv4 to adres, który został wyrejestrowany.

3256 Po zakończeniu wyrejestrowywania warstwa IPv4 może wysyłać pakiety IPv4 za pomocą adresu
3257 źródłowego.

3258 **5.4.8.4 Zarządzanie grupą multicast**

3259 **5.4.8.4.1 Ogólne**

3260 Ten rozdział opisuje prymitywy wykorzystywane do zarządzania grupami multicast.

3261 **5.4.8.4.2 CL_IPv4_IGMP_JOIN.request**

3262 Ten prymityw przekazywany jest z warstwy IPv4 do podwarstwy SSCS IPv4. Zawiera on adres multicast IPv4,
3263 do którego nastąpi dołączenie.

3264 Semantyka tego prymitywu przedstawia się następująco:

3265 *CL_IPv4_IGMP_JOIN.request{IPv4 }*

3266 Adres IPv4 to grupa multicast IPv4, do której ma nastąpić dołączenie.

3267 Gdy podwarstwa SSCS odbierze ten prymityw, będzie ona aranżować pakiety IPv4 wysyłane do tej grupy
3268 jako transmisje multicast w sieci OFDM PRIME i odbierać pakiety korzystające z tego adresu, które mają być
3269 przekazane do stosu IPv4. Jeśli podwarstwa CCSC IPv4 nie może dołączyć do grupy, korzysta ona z
3270 prymitywu CL_IPv4_IGMP.confirm. W przeciwnym razie do wskazania powodzenia stosowany jest prymityw
3271 CL_IPv4_IGMP_JOIN.confirm.

3272 5.4.8.4.3 CL_IPv4_IGMP_JOIN.confirm

3273 Ten prymityw przekazywany jest z podwarstwy SSCS IPv4 do warstwy IPv4. Zawiera on status wyniku oraz
3274 adres multicast IPv4, do którego dołączono.

3275 Semantyka tego prymitywu przedstawia się następująco:

3276 *CL_IPv4_IGMP_JOIN.confirm{IPv4}*

3277 Adres IPv4 to grupa multicast IPv4, do którego dołączono. SSCS IPv4 zacznie przekazywać pakiety multicast
3278 IPv4 dla danej grupy multicast.

3279 5.4.8.4.4 CL_IPv4_IGMP_LEAVE.request

3280 Ten prymityw przekazywany jest z warstwy IPv4 do podwarstwy SSCS IPv4. Zawiera on adres multicast IPv4,
3281 który ma zostać opuszczony.

3282 Semantyka tego prymitywu przedstawia się następująco:

3283 *CL_IPv4_IGMP_LEAVE.request{IPv4}*

3284 Adres IPv4 to grupa multicast IPv4, która będzie opuszczona. SSCS IPv4 zakończy przekazywanie pakietów
3285 multicast IPv4 dla danej tej grupy i może opuścić grupę multicast MAC OFDM PRIME.

3286 5.4.8.4.5 CL_IPv4_IGMP_LEAVE.confirm

3287 Ten prymityw przekazywany jest z podwarstwy SSCS IPv4 do warstwy IPv4. Zawiera on status wyniku oraz
3288 adres multicast IPv4, który został opuszczony.

3289 Semantyka tego prymitywu przedstawia się następująco:

3290 *CL_IPv4_IGMP_LEAVE.confirm{IPv4, Result}*

3291 Adres IPv4 to grupa multicast IPv4, która została opuszczona. SSCS IPv4 zakończy przekazywanie pakietów
3292 multicast IPv4 dla danej grupy multicast.

3293 Parametr *Result* przyjmuje wartość z Tabela 134.

3294 Ten prymityw może być stosowany przez podwarstwę SSCS jako wynik *CL_IPv4_IGMP_JOIN.request*,
3295 *CL_IPv4_IGMP_LEAVE.request* lub z powodu błędnego warunku prowadzącego do strat w połączeniu
3296 multicast OFDM PRIME MAC.

3297 5.4.8.5 Transfer danych**3298 5.4.8.5.1 Ogólne**

3299 Poniższe prymitywy stosowane są do wysyłania i odbierania pakietów IPv4.

3300 5.4.8.5.2 CL_IPv4_DATA.request

3301 Ten prymityw przekazywany jest z warstwy IPv4 do podwarstwy SSCS IPv4. Zawiera on jeden pakiet IPv4 do
3302 wysłania.

3303 Semantyka tego prymitywu przedstawia się następująco:

3304 *CL_IPv4_DATA.request{IPv4_PDU}*

3305 IPv4_PDU to pakiet IPv4 do wysłania.

3306 **5.4.8.5.3 CL_IPv4_DATA.confirm**

3307 Ten prymityw przekazywany jest z podwarstwy SSCS IPv4 do warstwy IPv4. Zawiera on wskazanie statusu i
3308 pakiet IPv4, który właśnie został wysłany.

3309 Semantyka tego prymitywu przedstawia się następująco:

3310 *CL_IPv4_DATA.confirm{IPv4_PDU, Result}*

3311 IPv4_PDU to pakiet IPv4, który miał zostać wysłany.

3312 Wartość *Wyniku* wskazuje czy pakiet został wysłany, czy wystąpił błąd. Przyjmuje on wartość z Tabela 134.

3313 **5.4.8.5.4 CL_IPv4_DATA.indicate**

3314 Ten prymityw przekazywany jest z podwarstwy SSCS IPv4 do warstwy IPv4. Zawiera on pakiet IPv4, który
3315 właśnie został odebrany.

3316 Semantyka tego prymitywu przedstawia się następująco:

3317 *CL_IPv4_DATA.indicate{IPv4_PDU}*

3318 IPv4_PDU to pakiet IPv4, który został odebrany.

3319 **5.5 IEC 61334-4-32 Podwarstwa konwergencji właściwa dla usługi** 3320 **(IEC 61334-4-32 SSCS)**

3321 **5.5.1 Ogólne**

3322 Dla wszystkich wymaganych usług, IEC 61334-4-32 SSCS obsługuje prymitywy DL_DATA zgodnie z normą IEC
3323 61334-4-32. Z normą IEC 61334-4-32 należy zapoznać się w tym samym czasie, jak z niniejszym punkcie,
3324 który nie stanowi samodzielnego tekstu.

3325 **5.5.2 Omówienie**

3326 Podwarstwa SSCS IEC 61334-4-32 zapewnia funkcje konwergencji dla aplikacji wykorzystujących usługi IEC
3327 61334-4-32. Wdrożenia zgodne z tą podwarstwą SSCS powinny oferować wszystkie podstawowe usługi LLC i
3328 usługi zarządzania LLC zgodnie z IEC 61334-4-32 (Wydanie z września 1996), podpunkty 2.2.1 i 2.2.3.
3329 Dodatkowo podwarstwa SSCS IEC 61334-4-32 podana w niniejszym punkcie zapewnia dodatkowe usługi,
3330 które pomagają mapować ten bezpołączeniowy protokół LLC IEC 61334-4-32 na zorientowaną na
3331 połączenie warstwę MAC.

- 3332 • Węzeł serwisowy może wymieniać dane tylko z węzłem podstawowym lub innymi węzłami
3333 serwisowymi. Spełnia to wymagania normy IEC 61334-4-32, która ma podobne ograniczenia.

- Każda sesja podwarstwy SSCS IEC 61334-4-32 ustanawia dedykowane połączenie OFDM PRIME MAC do wymiany danych unicast z węzłem podstawowym.
- Sesja SSCS węzła serwisowego odpowiada za inicjalizację tego połączenia do węzła podstawowego. SSCS węzła podstawowego nie może inicjować połączenia do węzła serwisowego.
- Każda podwarstwa SSCS IEC 61334-4-32 nasłuchuje połączenia broadcast MAC OFDM PRIME dedykowanego do przesyłania danych broadcast IEC 61334-4-32 z węzła podstawowego do węzłów serwisowych. Połączenie broadcast jest stosowane, gdy aplikacje w węźle podstawowym korzystające z usług IEC 61334-4-32 dokonują żądania transmisji z adresem docelowym *destination_address* stosowanym do transmisji broadcast lub gdy stosowane są funkcje broadcast SAP. W przypadku wielu sesji SSCS w obrębie węzła serwisowego, jedno połączenie broadcast warstwy MAC OFDM PRIME jest współdzielone przez wszystkie sesje SSCS.
- CPCS jest zawsze obecna przy sesji SSCS IEC 61334-4-32. Funkcjonalność podwarstwy SSCS opisano w punkcie 5.2.2. Tym samym MSDU wygenerowane przez SSCS IEC 61334-4-32 mają zawsze rozmiar mniejszy, niż *CLMTUSize* bajtów, a komunikaty aplikacji nie mogą być dłuższe niż *CLMaxAppPktSize*.

5.5.3 Alokacja adresu i nawiązywanie połączenia

Każde połączenie 4-32 będzie identyfikowane za pomocą unikalnego identyfikatora aplikacji, który będzie komunikować się przez to połączenie 4-32. Jest to zakres profilu komunikacji oparty na tych dolnych warstwach w celu zdefiniowania charakteru i zasad dla tego unikalnego identyfikatora. Informacje na temat unikalnego identyfikatora profilu DLMS/COSEM znajdują się w prTS/EN52056-8-4. Dla celów specyfikacji warstwy konwergencji 4-32 identyfikator ten będzie nazywany „Identyfikatorem urządzenia”.

Stos protokołów, jak określono w IEC 61334 definiuje adres docelowy identyfikujący każde urządzenie w sieci. Adres docelowy jest określony poza zakresem dokumentu IEC 61334-4-32. Jednakże, jest on stosowany przez dokument. Zatem aby urządzenia OFDM PRIME mogły korzystać z tej warstwy 4-32, wymagany jest również adres docelowy. Aby uzyskać więcej informacji na temat tego adresu docelowego należy zapoznać się z normą IEC 61334-4-1 punkt 4.3, Adresy MAC.

Adres docelowy ma zakres jednej podsieci OFDM PRIME. Warstwa SSCS 4-32 węzła podstawowego odpowiada za przydzielanie tych adresów dynamicznie i kojarzenie identyfikatora urządzenia sesji SSCS węzła serwisowego z przydzielonym adresem docelowym zgodnie z normą IEC-61334. Procedura jest następująca:

Gdy sesja węzła serwisowego IEC 61334-4-32 SSCS jest otwierana przez warstwę aplikacji, przekazuje ona identyfikator urządzenia. Sesja IEC 61334-4-32 SSCS następnie ustanawia swoje połączenie unicast do węzła podstawowego. To połączenie unicast wykorzystuje wartość *TYPE_CL_432* OFDM PRIME MAC, jak określono w Tabeli 132. Pakiet żądania połączenia wysłany z węzła serwisowego do węzła podstawowego zawiera parametry danych. Ten parametr danych zawiera identyfikator urządzenia. Format tych danych określono w punkcie 5.5.4.2.

Po odebraniu tego żądania połączenia w węźle podstawowym, węzeł podstawowy przydziela unikalny adres docelowej podsieci do sesji SSCS węzłów serwisowych. Węzeł podstawowy odsyła pakiet odpowiedzi na połączenie MAC PRIME OFDM, który zawiera parametr danych. Ten parametr danych zawiera przypisany adres docelowy i adres wykorzystywany przez węzeł podstawowy. Format tego parametru danych określono w punkcie 5.5.4.2. Prymityw 4-32 CL SAP stosowany jest w węźle podstawowym do wskazania

3374 mapowania sesji SSCS nowego węzła serwisowego identyfikatora urządzenia i adresu docelowego
3375 *destination_address* na aplikację 4-32 działającą węzle podstawowym.

3376 Po otrzymaniu ustanowienia połączenia i przekazaniu adresu docelowego w pakiecie ustanawiania
3377 połączenia MAC PRIME OFDM, sesja SSCS 4-32 potwierdza aplikacji, że sesja warstwy konwergencji została
3378 otwarta i wskazuje adres docelowy przypisany do sesji SSCS węzła serwisowego oraz adres węzła
3379 podstawowego. Węzeł serwisowy również otwiera połączenie broadcast OFDM PRIME MAC z LCID równym
3380 LCI_CL_432_BROADCAST, jak określono w Tabeli 133, jeśli żadna inna sesja SSCS nie otwierała już takiego
3381 połączenia broadcast. Połączenie to stosowane jest do dobierania pakietów broadcast wysyłanych przez
3382 warstwę konwergencji 4-32 węzła podstawowego do wszystkich sesji warstwy konwergencji węzła
3383 serwisowego.

3384 Jeśli węzeł podstawowy przydzielił wszystkie dostępne adresy docelowe, z powodu wyczerpania przestrzeni
3385 adresowej lub wartości granicznych wdrożenia, powinien on po prostu odrzucić żądanie połączenia z węzła
3386 serwisowego. Węzeł serwisowy może próbować ponownie ustanowić połączenie. Jednakże, aby uniknąć
3387 przeładowania podsieci PRIME OFDM takimi żądaniami, powinien on ograniczyć takie ustanawianie
3388 połączeń do jednej próby na minutę, gdy węzeł podstawowy odrzuca ustanawianie połączenia.

3389 Gdy połączenie unicast pomiędzy węzłem serwisowym a węzłem podstawowym zostanie zamknięte (np.
3390 ponieważ warstwa konwergencji w węzle serwisowym jest zamknięta lub połączenie poziomu warstwy
3391 MAC OFDM PRIME pomiędzy węzłem podstawowym a węzłem serwisowym zostało utracone), węzeł
3392 podstawowy oddzieli adres docelowy przypisany do sesji SSCS węzła serwisowego. Węzeł podstawowy
3393 użyje prymitywu 4-32 CL SAP (CL_432_LEAVE.indication) do wskazania dealokacji adresu docelowego z
3394 aplikacji 4-32 pracującej w węzle podstawowym.

3395 5.5.4 Format danych ustanawiania połączenia

3396 5.5.4.1 Ogólne

3397 Jak opisano w punkcie 5.5.3, dane połączenia PRIME OFDM MAC stosowane są do przenoszenia
3398 identyfikatora urządzenia do węzła podstawowego, a przypisanego adresu docelowego *destination_address*
3399 do sesji SSCS węzła serwisowego. Rozdział ten opisuje format stosowany dla tych danych.

3400 5.5.4.2 Węzeł serwisowy do Węzła podstawowego

3401 Sesja węzła serwisowego przekazuje identyfikator urządzenia do węzła podstawowego jako część
3402 połączenia. Format tego komunikatu pokazano w Tabeli 71.

3403 Tabela 71 - Dane sygnalizacji połączenia wysyłane przez węzeł serwisowy

Nazwa	Długość	Opis
Data.SN	n-oktetów	Identyfikator urządzenia. „Nazwa urządzenia logicznego COSEM” „Zarządzającego urządzenia logicznego” lub urządzenia DLMS/COSEM jak określono w DLMS/COSEM, które będzie komunikować się przez to połączenie 4-32.

5.5.4.3 Węzeł podstawowy do Węzła serwisowego

Węzeł podstawowy przekazuje przydzielony adres docelowy *destination_address* do sesji węzła serwisowego jako część żądania ustanawiania połączenia. Podaje on również swój własny adres węzłowi serwisowemu. Format tego komunikatu pokazano w Tabeli 72.

Tabela 72 - Dane sygnalizacji połączenia wysyłane przez węzeł podstawowy

Nazwa	Długość	Opis
<i>Reserved</i>	4 bity	Zarezerwowany. Powinien być kodowany jako zero dla tej wersji specyfikacji.
Data.DA	12 bitów	Adres docelowy przypisany do węzła serwisowego.
<i>Reserved</i>	4 bity	Zarezerwowany. Powinien być kodowany jako zero dla tej wersji specyfikacji.
Data.BA	12 bitów	Węzeł podstawowy wykorzystuje Base_address.

5.5.5 Format pakietu

Stosowane są formaty pakietów zgodnie z IEC 61334-4-32, Klauzula 4, Struktura jednostki danych protokołu LLC (LLC_PDU).

5.5.6 Punkt dostępu do usługi

5.5.6.1 Otwieranie i zamykanie warstwy konwergencji w Węźle serwisowym

5.5.6.1.1 CL_432_ESTABLISH.request

Ten prymityw jest przekazywany z aplikacji na warstwę konwergencji 4-32. Stosowany jest on do otwierania sesji warstwy konwergencji i inicjowania procesu rejestracji identyfikatora urządzenia w węźle podstawowym oraz przydzielania przez węzeł podstawowy adresu docelowego do sesji węzła serwisowego.

Semantyka tego prymitywu przedstawia się następująco:

CL_432_ESTABLISH.request{ DeviceIdentifier }

Identyfikator urządzenia jest identyfikatorem urządzenia, które ma zostać zarejestrowane w węźle podstawowym.

Jeśli identyfikator urządzenia jest zarejestrowany, a sesja warstwy konwergencji została skutecznie otwarta, używany jest prymityw CL_432_ESTABLISH.confirm. W przypadku wystąpienia błędu stosowany jest prymityw CL_432_RELEASE.confirm.

3426 5.5.6.1.2 CL_432_ESTABLISH.confirm

3427 Ten prymityw jest przekazywany z warstwy konwergencji 4-32 do aplikacji. Jest on używany do
3428 potwierdzania skutecznego otwarcia sesji warstwy konwergencji oraz potwierdzenia możliwości
3429 przekazywania danych przez warstwę konwergencji.

3430 Semantyka tego prymitywu przedstawia się następująco:

3431 *CL_432_ESTABLISH.confirm{ DeviceIdentifier, Destination_address, Base_address }*

3432

3433 Identyfikator urządzenia jest używany do identyfikacji, dla którego żądania CL_432_ESTABLISH.request jest
3434 potwierdzenie CL_432_ESTABLISH.confirm.

3435 Adres docelowy *destination_address* to adres przypisany do sesji 4-32 węzła serwisowego przez węzeł
3436 podstawowy.

3437 *Base_address* to adres wykorzystywany przez węzeł podstawowy.

3438 5.5.6.1.3 CL_432_RELEASE.request

3439 Ten prymityw jest przekazywany z aplikacji na warstwę konwergencji 4-32. Służy on do zamykania warstwy
3440 konwergencji i zwalniania wszystkich zasobów, które może przechować.

3441 Semantyka tego prymitywu przedstawia się następująco:

3442 *CL_432_RELEASE.request{Destination_address}*

3443 Adres docelowy *destination_address* to adres przypisany do sesji 4-32 węzła serwisowego, która ma zostać
3444 zamknięta.

3445 Warstwa konwergencji będzie stosować prymityw CL_432_RELEASE.confirm po zamknięciu sesji warstwy
3446 konwergencji.

3447 5.5.6.1.4 CL_432_RELEASE.confirm

3448 Ten prymityw jest przekazywany z warstwy konwergencji 4-32 do aplikacji. Prymityw informuje aplikację, że
3449 sesja warstwy konwergencji została zamknięta. Mogło tak się stać z powodu prymitywu żądania
3450 CL_432_RELEASE.request lub z powodu wystąpienia błędu, który wymusił zamknięcie sesji warstwy
3451 konwergencji.

3452 Semantyka tego prymitywu przedstawia się następująco:

3453 *CL_432_RELEASE.confirm{Destination_address, result}*

3454 Uchwyt połączenia identyfikuje sesję, która została zamknięta.

3455 Parametr *Result* ma znaczenie określone w Tabeli 134.

3456 **5.5.6.2 Otwieranie i zamykanie warstwy konwergencji w Węźle podstawowym**

3457 Dla otwierania i zamykania warstwy konwergencji w węźle podstawowym nie zdefiniowano żadnych
3458 prymitywów punktu dostępu do usług. Nie są wymagane żadne prymitywy, ponieważ aplikacja 4-32 w
3459 węźle podstawowym nie wymaga przekazywania jakichkolwiek informacji do warstwy konwergencji 4-32 w
3460 węźle podstawowym.

3461 **5.5.6.3 Wskazania węzła podstawowego**

3462 **5.5.6.3.1 Ogólne**

3463 Następujące prymitywy stosowane są w warstwie konwergencji 4-32 węzła podstawowego w celu
3464 wskazywania zdarzeń aplikacji 4-32 w węźle podstawowym. Wskazują one, gdy sesja węzła serwisowego
3465 dołączyła lub opuściła sieć.

3466 **5.5.6.3.2 CL_432_JOIN.indicate**

3467 *CL_432_JOIN.indicate{ Device Identifier, Destination_address}*

3468 Identyfikator urządzenia jest identyfikatorem urządzenia podłączonego do węzła serwisowego, które
3469 właśnie dołączyło do sieci.

3470 Adres docelowy to adres przypisany do węzła serwisowego przez węzeł podstawowy.

3471 **5.5.6.3.3 CL_432_LEAVE.indicate**

3472 *CL_432_LEAVE.indicate{Destination_address}*

3473 Adres docelowy to adres sesji węzła serwisowego, która właśnie opuściła sieć.

3474 **5.5.6.4 Prymitywy transferu danych**

3475 Prymitywy transferu danych stosowane są zgodnie ze specyfikacjami IEC 61334-4-32, punkty 2.2, 2.3, 2.4 i
3476 2.11. Jak wspomniano wcześniej, podwarstwa SSCS OFDM PRIME 432 wykorzystuje usługę IEC61334-4-32
3477 DL_Data (.req, .conf, .ind) do przesyłania wszystkich danych biorących udział w transferze.

3478

3479 **5.6 Podwarstwa konwergencji właściwa dla usługi IPv6 (SSCS IPv6)**

3480 **5.6.1 Omówienie**

3481 **5.6.1.1 Ogólne**

3482 Warstwa konwergencji IPv6 zapewnia skuteczną metodę przesyłania pakietów IPv6 przez sieć PRIME.

3483 Węzeł serwisowy może wysyłać pakiety IPv6 tylko do węzła podstawowego lub bezpośrednio do innych
3484 węzłów serwisowych.

3485 Domyślnie węzeł podstawowy działa jako router pomiędzy podsiecią PRIME, a siecią szkieletową. Wszystkie
3486 węzły podstawowe muszą mieć co najmniej tą możliwość dołączalności. Wszelkie inne węzły wewnątrz
3487 podsieci mogą również działać jako brama. Węzeł podstawowy może również działać jako router NAT.

3488 Jednak biorąc pod uwagę zagęszczenie adresów IPv6, nie jest to spodziewane. W jaki sposób węzeł
3489 podstawowy łączy się z siecią szkieletową wykracza poza zakres niniejszej specyfikacji.

3490 **5.6.1.2 Przypisanie adresowania unicast IPv6**

- 3491 • Węzły serwisowe IPv6 (lub węzły podstawowe) powinny obsługiwać standardowy protokół IPv6 jak
3492 opisano w RFC 2460.
- 3493 • Węzły serwisowe IPv6 (i węzły podstawowe) powinny obsługiwać standardową architekturę
3494 adresowania IPv6 jak opisano w RFC 4291.
- 3495 • Węzły serwisowe IPv6 (i węzły podstawowe) powinny obsługiwać globalne adresy IPv6 unicast,
3496 adresy IPv6 łącza lokalnego i adresy IPv6 multicast jak opisano w RFC 4291.
- 3497 • Węzły serwisowe IPv6 (lub węzły podstawowe) powinny obsługiwać automatyczną konfigurację
3498 adresów za pomocą bezstanowej konfiguracji adresu [RFC 2462]. Mogą one również obsługiwać
3499 automatyczną konfigurację adresu za pomocą stanowej konfiguracji adresu [RFC 3315], a także
3500 ręczną konfigurację adresów IPv6. Decyzja, który schemat konfiguracji adresu zastosować zależy od
3501 rozlokowania.
- 3502 • Węzeł serwisowy powinien obsługiwać klienta DHCPv6, gdy węzły obsługowe muszą obsługiwać
3503 serwer DHCPv6, jak opisano w RFC 3314 dla bezstanowej konfiguracji adresu.
- 3504

3505 **5.6.1.3 Zarządzanie adresami w podsieci PRIME**

3506 Pakiety routowane są w podsieci PRIME zgodnie z identyfikatorem węzła NID. Identyfikator węzła to
3507 połączenie identyfikatorów LNID i SID węzła serwisowego (patrz punkt 4.2). Węzeł podstawowy odpowiada
3508 za przypisywanie LNID do węzłów serwisowych. W czasie procesu rejestracji, który prowadzi do
3509 przydzielenia LNID do powiązanego węzła serwisowego, węzeł podstawowy rejestruje EUI-48 węzła
3510 serwisowego oraz przydzielony LNID wraz z SID.

3511 Na poziomie warstwy konwergencji adresowanie wykonywane jest za pomocą EUI-48 powiązanego węzła
3512 serwisowego. Rolą podwarstwy konwergencji jest konwersja adresu IPv6 w EUI-48 węzła serwisowego.
3513 Można to zrobić przy użyciu zestawu usług konwersji adresów węzła podstawowego.

3514 **5.6.1.4 Rola węzła podstawowego**

3515 Na poziomie podwarstwy konwergencji węzeł podstawowy zarządza tablicą zawierającą wszystkie adresy
3516 unicast IPv6 oraz odnoszący się do nich identyfikator EUI-48. Jedną z ról węzła podstawowego jest
3517 przeprowadzanie konwersji adresu IPv6 do EUI-48. Każdy węzeł serwisowy należący do podsieci zarządzanej
3518 przez węzeł podstawowy rejestruje swój adres IPv6 i adres EUI-48 w węźle podstawowym. Inne węzły
3519 serwisowe mogą następnie wysyłać zapytania do węzła podstawowego w celu konwersji adresu IPv6 na
3520 adres EUI-48. Wymaga to ustanowienia dedykowanego połączenia z węzłem podstawowym celem
3521 konwersji adresu: zarówno konwersji IPv4, jak i IPv6.

3522 Opcjonalnie nagłówki UDP/IPv6 można kompresować. Kompresja jest negocjowana jako część fazy
3523 ustanawiania połączenia. Aktualnie technologia kompresji jednego nagłówka opisana jest w niniejszej
3524 specyfikacji jako technika wykorzystywana do transmisji pakietów IPv6 w sieciach IEEE 802.15.4, zgodnie z
3525 RFC6282. Jest ona również zwana jako LOWPAN_IPHC1.

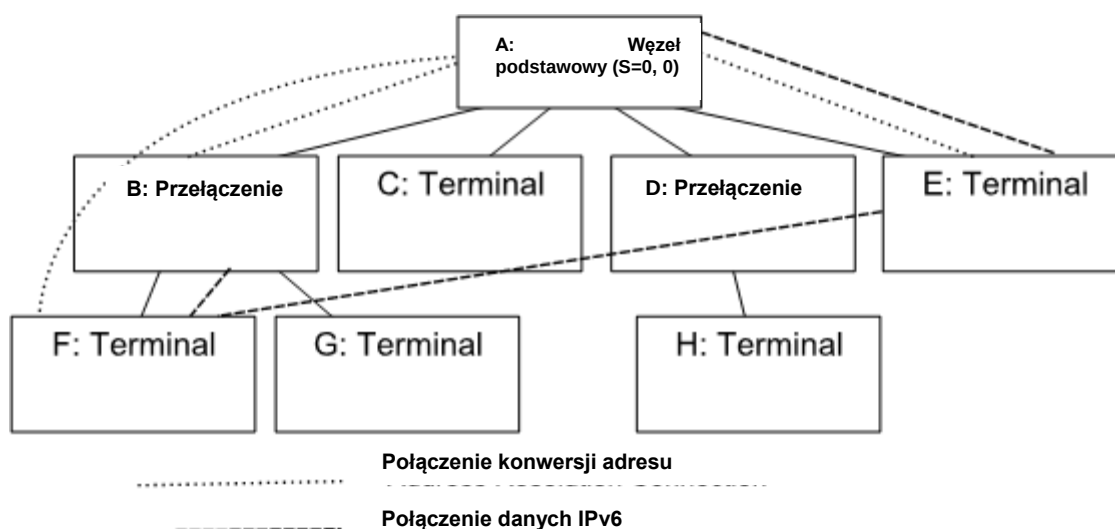
3526 Multicasting pakietów IPv6 jest obsługiwany za pomocą mechanizmu transmisji multicast MAC.

5.6.2 Warstwa konwergencji IPv6

5.6.2.1 Omówienie

5.6.2.1.1 Ogólne

Warstwa konwergencji posiada kilka typów połączeń. Dla konwersji adresu istnieje połączenie do węzła podstawowego. W przypadku transferu danych IPv6, na węzeł docelowy występuje jedno połączenie: z węzłem podstawowym, który działa jako bramka IPv6 do innych sieci lub do innego węzła w tej samej podsieci. Pokazano to na Rys. 99.



Rys. 99 – Przykład połączenia IPv6

W tym miejscu węzły B, E i F połączone są połączeniami konwersji adresu do węzła podstawowego. Węzeł E ma ustanowione połączenie danych z węzłem podstawowym i węzłem F. Węzeł F również połączony jest połączeniem danych z węzłem B. Rysunek nie pokazuje połączeń broadcast i multicast.

5.6.2.1.2 Routing w podsieci

Routing pakietów IPv6 leży w zakresie warstwy konwergencji. Innymi słowy, warstwa konwergencji zdecyduje czy pakiet powinien być wysłany bezpośrednio do innego węzła serwisowego lub przesłany do konfigurowanej bramy w zależności od adresu docelowego IPv6.

Mimo że IPv6 jest protokołem bezpołączeniowym, warstwa konwergencji IPv6 jest zorientowana na połączenie. Gdy konwersja adresu została już przeprowadzona, połączenie ustanowiono pomiędzy węzłem serwisowym źródłowym a węzłem docelowym do przesyłania pakietów IPv6. Połączenie to utrzymywane jest podczas transferu ruchu i może zostać usunięte po okresie braku aktywności.

5.6.2.1.3 Podział i scalanie

Podwarstwa CPCS powinna być zawsze obecna w warstwie konwergencji IPv6 dopuszczając podział i scalanie. Funkcjonalność podwarstwy SAR opisano w punkcie 5.2. Tym samym MSDU wygenerowane przez warstwę konwergencji IPv6 mają zawsze rozmiar mniejszy, niż CIMTUSize bajtów, a komunikaty aplikacji nie powinny być dłuższe niż CIMaxAppPktSize.

3552 **5.6.3 Konfiguracja adresu IPv6**

3553 **5.6.3.1 Omówienie**

3554 Węzły serwisowe mogą korzystać ze statystycznie skonfigurowanych adresów IPv6, adresów lokalnych
3555 łącza, stanowej lub bezstanowej konfiguracji zgodnie z RFC 2462 lub DHCPv6 w celu uzyskania adresów
3556 IPv6. Poza adresami skonfigurowanymi poniżej wszystkie węzły powinny obsługiwać adres lokalny łącza
3557 unicast oraz adresy multicast, jeśli węzeł będzie należał do grupy multicast.

3558 **5.6.3.2 Identyfikator interfejsu**

3559 W celu wykorzystania automatycznej bezstanowej konfiguracji adresu i adresów lokalnych łącza, konieczne
3560 jest zdefiniowanie sposobu wyprowadzania identyfikatora interfejsu zgodnie z RFC4291. Każdy węzeł
3561 PRIME posiada unikalny identyfikator EUI-48. Ten identyfikator EUI-48 jest konwertowany w EUI-64 w taki
3562 sam sposób, jak dla sieci Ethernet zgodnie z RFC2464. EUI-64 jest następnie stosowany jako identyfikator
3563 interfejsu.

3564 **5.6.3.3 Konfiguracja adresu połączenia lokalnego IPv6**

3565 Adres lokalny łącza IPv6 interfejsu PRIME tworzy się poprzez dołączenie identyfikatora interfejsu do
3566 prefiksu FE80::/64.

3567 **5.6.3.4 Bezstanowa konfiguracja adresu**

3568 Prefiks adresu IPv6 stosowany dla bezstanowej konfiguracji automatycznej interfejsu PRIME, zgodnie z
3569 RFC4862, powinien mieć długość 64 bitów. Prefiks IPv6 uzyskiwany jest przez węzły serwisowe z węzła
3570 podstawowego za pośrednictwem komunikatów Router Advertisement, które są wysyłane okresowo lub na
3571 żądanie węzła podstawowego.

3572 **5.6.3.5 Stanowa konfiguracja adresu**

3573 Adres IPv6 może być alternatywnie skonfigurowany za pomocą DHCPv6, jak opisano w RFC 3315. DHCPv6
3574 może dostarczyć urządzeniu adresy przypisane przez serwer DHCPv6 oraz inne informacje o konfiguracji,
3575 które przenoszone są opcjonalnie.

3576 **5.6.3.6 Adres multicast**

3577 Węzły serwisowe IPv6 (i węzły podstawowe) powinny obsługiwać adresowanie IPv6 multicast jak opisano w
3578 RFC 4291, punkt 2.7.

3579 **5.6.3.7 Konwersja adresu**

3580 **5.6.3.7.1 Omówienie**

3581 Warstwa IPv6 dostarczy warstwie konwergencji IPv6 pakiet IPv6 do przesłania. Warstwa konwergencji
3582 odpowiada za określenie, do którego węzła serwisowego dostarczony powinien zostać pakiet za pomocą
3583 adresów IPv6 w tym pakiecie. Warstwa konwergencji musi następnie ustanowić połączenie z węzłem
3584 docelowym jeśli takie jeszcze nie istnieje, tak aby pakiet można było przesłać. Stosować można dwie klasy
3585 adresów IPv6, a następny punkt opisuje sposób konwersji tych adresów na adresy EUI-48 PRIME. Należy
3586 zauważyć, że IPv6 nie posiada adresu broadcast. Jednak nadawanie broadcast jest możliwe przy użyciu
3587 wszystkich adresów węzłów.

3588

3589 **5.6.3.7.2 Adres Unicast**3590 **5.6.3.7.2.1 Ogólne**

3591 Adresy unicast IPv6 muszą zostać przekonwertowane na adresy unicast EUI-48 PRIME. Węzeł podstawowy
3592 zarządza centralną bazą danych adresów IPv6 węzła i adresów EUI-48. Funkcje konwersji adresu są
3593 przeprowadzane poprzez wysyłanie do tej bazy danych zapytań. Węzeł serwisowy musi ustanowić
3594 połączenie z usługą konwersji adresów pracującą na węźle podstawowym za pomocą wartości typu
3595 połączenia TYPE_CL_IPv6_AR. Żadne dane nie powinny być przekazywane w sygnalizowaniu nawiązania
3596 połączenia. Za pomocą tego połączenia węzeł serwisowy może skorzystać z dwóch mechanizmów
3597 określonych w niniejszej specyfikacji.

3598

3599 **5.6.3.7.2.2 Rejestrowanie i wyrejestrowywanie adresu**

3600 Węzeł serwisowy stosuje komunikat AR_REGISTERv6_S do zarejestrowania adresu IPv6 i odpowiadającego
3601 mu adresu EUI-48. Węzeł podstawowy zatwierdzi komunikat AR_REGISTERv6_B. Węzeł serwisowy może
3602 zarejestrować wiele adresów IPv6 dla tego samego adresu EUI-48.

3603 Węzeł serwisowy stosuje komunikat AR_UNREGISTERv6_S do wyrejestrowania adresu IPv6 i
3604 odpowiadającego mu adresu EUI-48. Węzeł podstawowy zatwierdzi komunikat AR_UNREGISTERv6_B.

3605 Gdy połączenie konwersji adresu pomiędzy węzłem serwisowym, a węzłem podstawowym zostanie
3606 zamknięte, węzeł podstawowy usunie wszystkie adresy powiązane z tym połączeniem.

3607

3608 **5.6.3.7.2.3 Wyszukiwanie adresu**

3609 Węzeł serwisowy korzysta z komunikatu AR_LOOKUPv6_S do przeprowadzania wyszukiwania. Komunikat
3610 zawiera adres IPv6 do konwersji. Węzeł podstawowy odpowie za pomocą komunikatu AR_LOOKUPv6_B,
3611 który zawiera kod błędu i, jeśli nie ma żadnych błędów, adres EUI-48 powiązany z adresem IPv6. Jeśli węzeł
3612 podstawowy ma wiele wpisów w swojej bazie danych dla tego samego adresu IPv6, możliwy zwrócony
3613 adres EUI-48 nie jest zdefiniowany.

3614 Należy zauważyć, że w przypadku adresów lokalnych łączy, w wyniku faktu, że EUI-48 można uzyskać z
3615 adresu IPv6, wyszukiwanie może po prostu zwrócić tę wartość poprzez wyodrębnienie jej z adresu IPv6.

3616 **5.6.3.7.3 Adres multicast**

3617 Adresy multicast IPv4 mapowane są na uchwyt połączenia (*ConHandle*) przez warstwę konwergencji.

3618 Aby dołączyć do grupy multicast, warstwa konwergencji korzysta z prymitywu MAC_JOIN.request z
3619 adresem IPv6 określonym w polu danych. Odpowiedni prymityw MAC_JOIN.Confirm zostanie
3620 wygenerowany przez MAC po zakończeniu procesu dołączania. Prymityw MAC_Join.Confirm będzie
3621 zawierał wynik (powodzenie/niepowodzenie) oraz odpowiedni parametr *ConHandle* używany przez
3622 warstwę konwergencji. Warstwa MAC zajmie się transferem danych dla tego połączenia za pomocą

3623 odpowiednich identyfikatorów LCID. Aby opuścić grupę multicast warstwa konwergencji w węźle
3624 serwisowym powinna użyć prymitywu MAC_LEAVE.request [ConHandle].

3625 Aby wysłać pakiet multicast IPv6, warstwa konwergencji po prostu wyśle pakiet do grupy za pomocą
3626 przypisanego *ConHandle*. Parametr *ConHandle* jest utrzymywany, jeśli do wysłania pozostały jeszcze
3627 pakiety. Jednakże, po upływie *Tmcast_reg* sekund niewysyłania pakietu multicast IPv6 do grupy, węzeł
3628 powinien zwolnić parametr *ConHandle* za pomocą prymitywu MAC_LEAVE.request. Wartość nominalna
3629 *Tmcast_reg* to 10 minut, jednakże stosować można inne wartości.

3630 5.6.3.7.4 Retransmisja pakietów konwersji adresu

3631 Połączenie pomiędzy węzłem serwisowym a węzłem podstawowym dla konwersji adresu nie jest
3632 niezawodne. ARQ MAC nie jest używane. Węzeł serwisowy do retransmisji jeśli węzeł podstawowy nie
3633 odpowiada w ciągu jednej sekundy. Nie jest błędem, gdy węzeł podstawowy otrzymuje te same żądania
3634 rejestracji kilka razy lub jest proszony o usunięcie rejestracji, która nie istnieje. Warunki te mogą być
3635 wynikiem retransmisji.

3636 5.6.4 Transfer pakietu IPv6

3637 Dla pakietów do przeniesienia należy ustanowić połączenie pomiędzy węzłem źródłowym a docelowym.
3638 Warstwa konwergencji IPv6 sprawdzi każdy pakiet IP, aby określić docelowy adres EUI-48. Jeśli połączenie z
3639 punktem docelowym zostało już ustanowione, pakiet jest po prostu wysyłany. Aby tego dokonać, warstwa
3640 konwergencji zarządza tabelą dla każdego połączenia zawierającą informacje podane w Tabeli 73. Aby
3641 skorzystać z tej tabeli, konieczne jest określenie czy adres zdalny znajduje się w lokalnej podsieci lub czy
3642 należy użyć bramki. W tym celu stosowana jest maska podsieci skojarzona z lokalnym adresem IPv6. Jeśli
3643 adres docelowy nie znajduje się w lokalnej podsieci, podczas przeszukiwania tabeli zamiast adresu
3644 docelowego stosowany jest adres bramy.

3645 Tabela 73 – Pozycje tablicy warstwy konwergencji IPv6

Parametr	Opis
CL_IPv6_Con.Remote_IP	Zdalny adres IP tego połączenia
CL_IPv6_Con.ConHandle	Uchwyt połączenia MAC dla połączenia
CL_IPv6_Con.LastUsed	Data i czas ostatniego odebranego/wysłanego pakietu
CL_IPv6_Con.HC	Stosowany schemat kompresji nagłówka

3646 Warstwa konwergencji może zamknąć połączenie, gdy nie zostało ono wykorzystane do określonego przez
3647 realizację okresu czasu. Kiedy połączenie jest zamykane, wejście do podłączenia jest usuwane na obu
3648 końcach połączenia.

3649 Gdy połączenie do miejsca przeznaczenia nie istnieje, konieczne są dodatkowe prace. Usługa konwersji
3650 adresu stosowana jest do określenia adresu EUI-48 zdanego adresu IPv6 jeśli jest on adresem lokalnym lub
3651 bramy skojarzonej z lokalnym adresem jeśli adres docelowy znajduje się w kolejnej podsieci. Jeśli węzeł
3652 podstawowy odpowiada za pomocą adresu EUI-48 docelowego węzła serwisowego, ustanawiane jest
3653 połączenie MAC ze zdalnym urządzeniem. Wartość TYPE tego połączenia to TYPE_CL_IPv6_UNICAST. Dane

3654 przekazywane w komunikacie żądania określono w punkcie 5.6.8.3. Lokalny adres IPv6 jest podawany po to,
3655 aby zdalne urządzenie mogło dodać nowe połączenie do pamięci podręcznej połączeń do przesyłania
3656 danych w przeciwnym kierunku. Korzystanie z kompresji nagłówków jest również wynegocjowane w
3657 ramach ustanawiania połączenia. Po nawiązaniu połączenia, pakiety IPv6 mogą być wysyłane.

3658 5.6.5 Podział i scalanie

3659 Warstwa konwergencji IPv6 powinna obsługiwać pakiety IPv6 przy MTU wynoszącej 1500 bajtów. Wymaga
3660 to zastosowania usługi podziału i scalania wspólnej warstwy konwergencji.

3661

3662 5.6.6 Kompresja

3663 Zakłada się, że każde urządzenie PRIME potrafi kompresować/dekompresować nagłówek IPv6
3664 LOWPAN_IPHC. Może ono także przeprowadzać kompresję/dekompresję UDP. Tak więc kompresja
3665 UDP/IPv6 jest negocjowana.

3666 W przypadku pakietu multicast nie mają miejsca negocjacje. Węzły mogą korzystać tylko z obowiązkowych
3667 możliwości kompresji

3668 W zależności od typu adresu IPv6 przenoszonego przez pakiet i uprawnień wynegocjowanych przez węzły
3669 biorące udział w wymianie danych, przeprowadzana jest kompresja nagłówka IPv6.

3670 Wszystkie węzły serwisowe i węzeł podstawowy powinny obsługiwać kompresję nagłówka IPv6 za pomocą
3671 bezstanowej kompresji adresów źródłowych i docelowych zgodnie z RFC 6282. Źródłowe i docelowe adresy
3672 IPv6 korzystające z kompresji stanowej oraz kompresji kolejnego nagłówka IPv6 są negocjowane.

3673 5.6.7 Mapowanie jakości usług

3674 MAC PRIME określa czy mechanizm współdzielonej kontencji obsługuje 4 poziomy priorytetów (1-4).
3675 Poziom 1 stosowany jest dla wiadomości sygnalizacyjnych MAC, ale nie tylko.

3676 Pakiety IPv6 zawierają w nagłówku pole Klasy ruchu w celu wskazania jakości usługi, jaką pakiet chciałby
3677 otrzymać. Ta klasa ruchu może być stosowana w taki sam sposób jak TOS IPv4 (patrz [7]). Znaczący to, że trzy
3678 bity TOS wskazują priorytet IP. Poniższa tabela określa sposób mapowania priorytetu IP na
3679 priorytet MAC PRIME.

3680

Tabela 74 – Mapowanie priorytetu IPv6 na priorytet MAC PRIME

Priorytet IP	Priorytet MAC
000 – Ruch zwyczajny	4
001 – Ruch nadrzędny	4
010 – Ruch natychmiastowy	3
011 – Ruch błyskawiczny	3

100 – Ruch ponadświetlny	2
101 – Ruch krytyczny	2
110 – Ruch kontroli intersieci WAN	1
111 – Ruch kontroli sieci	1

3681

3682 **Uwaga:** Na poziomie warstwy MAC priorytet podany w polu nagłówka pakietu jest wartością przypisywaną
3683 w tej tabeli minus 1, ponieważ zakres pola PKT.PRIO wynosi od 0 do 3.

3684 5.6.8 Formaty pakietów i dane połączenia

3685 5.6.8.1 Omówienie

3686 Punkt ten określa format jednostek PDU warstwy konwergencji.

3687 5.6.8.2 PDU konwersji adresu

3688 5.6.8.2.1 Ogólne

3689 Kolejne PDU są przesyłane za pomocą połączenia konwersji adresu pomiędzy węzłem serwisowym, a
3690 węzłem podstawowym. Poniższe punkty definiują kilka wartości AR.MSG. Wszystkie inne wartości są
3691 zarezerwowane dla nowszych wersji tej specyfikacji.

3692

3693 5.6.8.2.2 AR_REGISTERv6_S

3694 Tabela 75 pokazuje komunikat rejestracji konwersji adresu wysłany z węzła serwisowego do węzła
3695 podstawowego.

3696

Tabela 75 - Format komunikatu AR_REGISTERv6_S

Nazwa	Długość	Opis
AR.MSG	8 bitów	Typ komunikatu konwersji adresu Dla AR_REGISTERv6_S = 16
AR.IPv6	128 bitów	Adres IPv4 do zarejestrowania
AR.EUI-48	48 bitów	EUI-48 do zarejestrowania

3697 **AR_REGISTERv6_B**

3698 Tabela 76 pokazuje komunikat zatwierdzenia rejestracji konwersji adresu wysłany z węzła podstawowego
3699 do węzła serwisowego.

3700 **Tabela 76 - Format komunikatu AR_REGISTERv6_B**

Nazwa	Długość	Opis
AR.MSG	8 bitów	Typ komunikatu konwersji adresu Dla AR_REGISTERv6_B = 17
AR.IPv6	128 bitów	Zarejestrowany adres IPv6
AR.EUI-48	48 bitów	EUI-48 zarejestrowany

3701

3702 Pola AR.IPv6 i AR.EUI-48 są ujęte w komunikacie AR_REGISTERv6_B, więc węzeł serwisowy może
3703 przeprowadzać wiele nakładających się na siebie rejestracji.

3704

3705 **5.6.8.2.3 AR_UNREGISTERv6_S**

3706 Tabela 77 pokazuje komunikat wyrejestrowania konwersji adresu wysłany z węzła serwisowego do węzła
3707 podstawowego.

3708 **Tabela 77 - format komunikatu AR_UNREGISTERv6_S**

Nazwa	Długość	Opis
AR.MSG	8 bitów	Typ komunikatu konwersji adresu Dla AR_UNREGISTERv6_S = 18
AR.IPv6	128 bitów	Adres IPv6 do wyrejestrowania
AR.EUI-48	48 bitów	EUI-48 do wyrejestrowania

3709 **5.6.8.2.4 AR_UNREGISTERv6_B**

3710 Tabela 78 pokazuje komunikat zatwierdzenia wyrejestrowania konwersji adresu wysłany z węzła
3711 podstawowego do węzła serwisowego.

3712 Tabela 78 - format komunikatu AR_UNREGISTERv6_B

Nazwa	Długość	Opis
AR.MSG	8 bitów	Typ komunikatu konwersji adresu Dla AR_UNREGISTERv6_B = 19
AR.IPv6	128 bitów	Wyrejestrowany adres IPv6
AR.EUI-48	48 bitów	EUI-48 wyrejestrowany

3713 Pola AR.IPv6 i AR.EUI-48 są ujęte w komunikacie AR_UNREGISTERv6_B, więc węzeł serwisowy może
3714 przeprowadzać wiele nakładających się na siebie wyrejestrowań.

3715

3716 5.6.8.2.5 AR_LOOKUPv6_S

3717 Tabela 79 pokazuje komunikat wyszukiwania konwersji adresu wysłany z węzła serwisowego do węzła
3718 podstawowego.

3719 Tabela 79 - format komunikatu AR_LOOKUPv6_S

Nazwa	Długość	Opis
AR.MSG	8 bitów	Typ komunikatu konwersji adresu Dla AR_LOOKUPv6_S = 20
AR.IPv6	128 bitów	Adres IPv6 do wyszukania

3720

3721 5.6.8.2.6 AR_LOOKUPv6_B

3722 Tabela 80 pokazuje komunikat wyszukiwania konwersji adresu wysłany z węzła podstawowego do węzła
3723 serwisowego.

3724 Tabela 80 - format komunikatu AR_LOOKUPv6_B

Nazwa	Długość	Opis
AR.MSG	8 bitów	Typ komunikatu konwersji adresu Dla AR_LOOKUPv6_B = 21
AR.IPv6	128 bitów	Wyszukany adres IPv6

AR.EUI-48	48 bitów	EUI-48 dla adresu IPv6
AR.Status	8 bitów	Status wyszukiwania wskazujący czy adres został znaleziony, czy też wystąpił błąd. 0 = znaleziony, AR.EUI-48 prawidłowy. 1 = nieznan, AR.EUI-48 niezdefiniowany

Wyszukiwanie może nie powieść się, jeśli żądany adres nie został zarejestrowany. W tym przypadku AR.Status będzie miał wartość równą 1, a treść AR.EUI-48 będzie niezdefiniowana. Wyszukiwanie jest skuteczne jedynie, gdy AR.Status wynosi zero. W tym przypadku EUI-48 zawiera przekonwertowany adres.

3728

3729 5.6.8.2.7 AR_MCAST_REGv6_S

3730 Tabela 81 pokazuje komunikat rejestracji konwersji adresu multicast wysłany z węzła serwisowego do węzła podstawowego.

3732 Tabela 81 - format komunikatu AR_MCAST_REGv6_S

Nazwa	Długość	Opis
AR.MSG	8 bitów	Typ komunikatu konwersji adresu Dla AR_MCAST_REGv6_S = 24
AR.IPv6	128 bitów	Adres multicast IPv6 do zarejestrowania.

3733

3734 5.6.8.2.8 AR_MCAST_REGv6_B

3735 Tabela 82 pokazuje komunikat rejestracji konwersji adresu multicast wysłany z węzła podstawowego do węzła serwisowego.

3737 Tabela 82 - format komunikatu AR_MCAST_REGv6_B

Nazwa	Długość	Opis
AR.MSG	8 bitów	Typ komunikatu konwersji adresu Dla AR_MCAST_REGv6_B = 25
AR.IPv6	128 bitów	Zarejestrowany adres multicast IPv6
<i>Reserved</i>	2 bity	Zarezerwowany. Powinien być kodowany jako 0.

AR.LCID	6 bitów	Identyfikator połączenia lokalnego przypisany do tego adresu IPv6 multicast
---------	---------	---

3738 Pole AR.IPv6 jest ujęte w komunikacie AR_MCAST_REG_B, więc węzeł serwisowy może przeprowadzać
3739 wiele nakładających się na siebie rejestracji.

3740 5.6.8.2.9 AR_MCAST_UNREGv6_S

3741 Tabela 83 pokazuje komunikat wyrejestrowania konwersji adresu multicast wysłany z węzła serwisowego
3742 do węzła podstawowego.

3743 Tabela 83 - format komunikatu AR_MCAST_UNREGv6_S

Nazwa	Długość	Opis
AR.MSG	8 bitów	Typ komunikatu konwersji adresu Dla AR_MCAST_UNREGv6_S = 26
AR.IPv6	128 bitów	Adres multicast IPv6 do wyrejestrowania.

3744

3745 5.6.8.2.10 AR_MCAST_UNREGv6_B

3746 Tabela 84 pokazuje komunikat wyrejestrowania konwersji adresu multicast wysłany z węzła podstawowego
3747 do węzła serwisowego.

3748 Tabela 84 - format komunikatu AR_MCAST_UNREGv6_B

Nazwa	Długość	Opis
AR.MSG	8 bitów	Typ komunikatu konwersji adresu Dla AR_MCAST_UNREGv6_B = 27
AR.IPv6	128 bitów	Wyrejestrowany adres multicast IPv6

3749 Pole AR.IPv6 jest ujęte w komunikacie AR_MCAST_UNREGv6_B, więc węzeł serwisowy może
3750 przeprowadzać wiele nakładających się na siebie wyrejestrowań.

3751 5.6.8.3 Format pakietu IPv6

3752 5.6.8.3.1 Ogólne

3753 Następujące formaty PDU stosowane są do przesyłania pakietów IPv6 pomiędzy węzłami serwisowymi.

3754

3755 5.6.8.3.2 Brak wynegocjowanej kompresji nagłówka

3756 Jeśli kompresja nagłówka nie występuje, pakiet IPv6 wysyłany jest w takim stanie, bez nagłówka.

3757 Tabela 85 - Format pakietu IPv6 bez wynegocjowanej kompresji nagłówków

Nazwa	Długość	Opis
IPv6.PKT	n-oktetów	Pakiet IPv6

3758 5.6.8.3.3 Kompresja nagłówka

3759 Podczas kompresji nagłówka LOWPAN_IPHC1 i negocjowania kompresji kolejnego nagłówka, pakiet
3760 UDP/IPv6 wysyłany jest zgodnie z Tabela 86.

3761 Tabela 86 - Format pakietu UDP/IPv6 z kompresją nagłówków LOWPAN_IPHC1 i LOWPAN_NHC

Nazwa	Długość	Opis
IPv6.IPHC	2 oktety	Wysyłanie + kodowanie LOWPAN_IPHC. Z bitem 5=1 wskazującym, że kolejny bit jest skompresowany za pomocą formatu LOWPAN_NHC.
IPv6.ncIPv6	n.m-oktetów	Nieskompresowane pola IPv6
IPv6.HC_UDP	1 oktet	Kodowanie następnego nagłówka
IPv6.ncUDP	n.m-oktetów	Nieskompresowane pola UDP
Wypełnienie	0.m-oktetów	Wypełnienie do granicy bajta
IPv6.DATA	n-oktetów	Dane UDP

3762 Należy zauważyć, że te pola nie są konieczne wyrównane do wielokrotności bajtowych. Na przykład pole
3763 IPv6.ncIPv6 może mieć dowolną liczbę bitów. Pole IPv6.IPHC_UDP następuje bezpośrednio po nim, bez
3764 żadnego wypełniania. Wypełnienie stosowane jest jedynie na końcu pełnego skompresowanego nagłówka
3765 UDP/IPv6, tak że dane są wyrównane do wielokrotności bajtowych.

3766 Gdy pakiet IPv6 zawiera dane inne niż UDP, stosowany jest następujący format pakietu pokazany w **Błąd!**
3767 **Nie można odnaleźć źródła odwołania..**

3768 Tabela 87 - Format pakietu IPv6 z wynegocjowaną kompresją nagłówków LOWPAN_IPHC

Nazwa	Długość	Opis
-------	---------	------

IPv6.IPHC	2 oktety	Kodowanie HC. Bity 5 zawierają 0, co oznacza, że kolejny bajt nagłówka nie jest skompresowany.
IPv6.ncIPv6	n.m-oktetów	Nieskompresowane pola IPv6
Wypełnienie	0.m-oktetów	Wypełnienie do granicy bajta
IPv6.DATA	n-oktetów	Dane protokołu internetowego

3769 5.6.8.4 Dane połączenia

3770 5.6.8.4.1 Omówienie

3771 Gdy pomiędzy węzłami serwisowymi nawiązano połączenie do przesyłania pakietów IPv6, dane przesyłane
 3772 są również w pakietach żądania połączenia. Dane te pozwalają na negocjacje kompresji i powiadomienie
 3773 adresu IPv6.

3774

3775 5.6.8.4.2 Dane połączenia od inicjatora

3776 Tabela 88 pokazuje dane połączenia wysyłane przez inicjatora.

3777 Tabela 88 - Dane sygnalizacji połączenia IPv6 wysyłane przez inicjatora

Nazwa	Długość	Opis
<i>Reserved</i>	6 bitów	Powinien być kodowany jako zero w tej wersji protokołu warstwy konwergencji
Data.HCNH	2 bity	Kompresja nagłówka wynegocjowana • Data.HC = 0 – Brak żądania kompresji • Data.HC = 1 – LOWPAN_NH • Data.HC = 2 – stanowa kompresja adresu. • Data.HC = 3 – LOWPAN_NH i stanowa kompresja adresu.
Data.IPv6	128 bitów	Adres IPv6 inicjatora.

3778 Jeśli urządzenie przyjmuje połączenie, powinno one skopiować adres Data.IPv6 do nowej pozycji tablicy
 3779 wraz z wynegocjowaną wartością Data.HC.

3780

3781 5.6.8.4.3 Dane połączenia od respondenta

3782 Tabela 89 pokazuje dane połączenia wysyłane w odpowiedzi na żądanie połączenia.

3783 Tabela 89 - Dane sygnalizacji połączenia IPv6 wysyłane przez respondenta

Nazwa	Długość	Opis
<i>Reserved</i>	6 bitów	Powinien być kodowany jako zero w tej wersji protokołu warstwy konwergencji
Data.HC	2 bity	Kompresja nagłówka wynegocjowana - Data.HC = 0 – Brak żądania kompresji: UWAGA: Gdy stosowana jest bezstanowa kompresja adresu, obsługiwać powinny ją wszystkie węzły. Jeśli bezstanowa kompresja adresów nie jest stosowana, węzeł za pomocą tej wartości poinformuje o swoich uprawnieniach do kompresji. Data.HC = 1 – LOWPAN_NH - Data.HC = 2 – stanowa kompresja adresu. - Data.HC = 3 – LOWPAN_NH i stanowa kompresja adresu.

3784 Wszystkie węzły obsługują bezstanową kompresję adresu.

3785 Schemat kompresji kolejnego nagłówka i stanowa kompresja adresu mogą być zastosowane wyłącznie, jeśli
3786 obsługiwany jest przez węzły serwisowe. Respondent może jedynie ustawić Data.HC na tę samą wartość,
3787 jak wartość odebrana od inicjatora lub wartość niższą niż wartość odebrana. Gdy stosowana jest ta sama
3788 wartość, wskazuje ona, że żądany schemat kompresji został wynegocjowany i będzie stosowany dla tego
3789 połączenia. Ustawienie Data.HC na niższą wartość pozwala respondentowi na odmówienie żądania dla tego
3790 schematu kompresji nagłówka.

3791 5.6.9 Punkt dostępu do usługi

3792 5.6.9.1 Omówienie

3793 Ten punkt określa punkt dostępu do usług stosowany przez warstwę IPv6 do komunikowania się z warstwą
3794 konwergencji IPv6.

3795 5.6.9.2 Otwieranie i zamykanie warstwy konwergencji

3796 Poniższe prymitywy stosowane są do otwierania i zamykania warstwy konwergencji. Warstwa konwergencji
3797 może zostać otwarta tylko raz. Warstwa IPv6 może zamknąć warstwę konwergencji, gdy interfejs IPv6
3798 zostanie zamknięty. IPv6 również zamknie warstwę konwergencji, gdy podstawowe połączenie MAC do
3799 węzła podstawowego zostało utracone.

3800

3801 5.6.9.2.1 CL_IPv6_Establish.request

3802 Prymityw CL_IPv6_ESTABLISH.request jest przekazywany z warstwy IPv6 do warstwy konwergencji IPv6.
3803 Stosowany jest, gdy warstwa IPv6 przenosi interfejs w górę.

3804 Semantyka tego prymitywu przedstawia się następująco:

3805 *CL_IPv6_ESTABLISH.request{}*

3806 Po odebraniu tego prymitywu warstwa konwergencji utworzy połączenie konwersji adresu do węzła
3807 podstawowego.

3808

3809 5.6.9.2.2 CL_IPv6_Establish.confirm

3810 Prymityw CL_IPv6_ESTABLISH.confirm jest przekazywany z warstwy konwergencji IPv6 do warstwy IPv6.
3811 Stosowany jest do wskazania, czy podwarstwa konwergencji jest gotowa do uzyskania dostępu do pakietów
3812 IPv6 przesyłanych do warstw równorzędnych.

3813 Semantyka tego prymitywu przedstawia się następująco:

3814 *CL_IPv6_ESTABLISH.confirm{}*

3815 Gdy warstwa konwergencji ustanowi wszystkie niezbędne połączenia i jest gotowa na przesłanie i
3816 odbieranie pakietów IPv6, prymityw ten przekazywany jest do warstwy IPv6. Jeśli warstwa konwergencji
3817 IPv6 napotka na błąd podczas otwierania, odpowie ona za pomocą prymitywu CL_IPv6_RELEASE.confirm, a
3818 nie prymitywu CL_IPv6_ESTABLISH.confirm.

3819

3820 5.6.9.2.3 CL_IPv6_Release.request

3821 Prymityw CL_IPv6_RELEASE.request stosowany jest przez warstwę IPv6, gdy interfejs jest zamknięty.
3822 Warstwa konwergencji zamyka wszystkie połączenia tak, aby żadne inne pakiety IPv6 nie były
3823 otrzymywane, a wszystkie inne zasoby zostały zwolnione.

3824 Semantyka tego prymitywu przedstawia się następująco:

3825 *CL_IPv6_RELEASE.request{}*

3826 Gdy warstwa konwergencji zwolni wszystkie swoje połączenia i zasoby, zwróci prymityw
3827 CL_IPv6_RELEASE.confirm.

3828

3829 5.6.9.2.4 CL_IPv6_Release.confirm

3830 Prymityw CL_IPv6_RELEASE.confirm stosowany jest przez warstwę konwergencji IPv6 do wskazywania
3831 warstwie IPv6, że warstwa IPv6 została zamknięta. Może nastąpić to w wyniku prymitywu
3832 CL_IPv6_RELEASE.request prymitywu CL_IPv6_ESTABLISH.request lub ponieważ warstwa MAC wskazuje, że
3833 połączenie konwersji adresu zostało utracone lub sam węzeł serwisowy nie jest już zarejestrowany.

3834 Semantyka tego prymitywu przedstawia się następująco:

3835 CL_IPv6_RELEASE.confirm{result}

3836 Parametr Result ma znaczenie określone w Tabeli 118.

3837

3838 5.6.9.3 Zarządzanie adresem Unicast

3839 5.6.9.3.1 Ogólne

3840 Opisane tu prymitywy są stosowane do zarządzania adresami, tj. rejestracji i wyrejestrowywania adresów
3841 IPv6 powiązanych z tą warstwą konwergencji.

3842 W przypadku braku adresów IPv6 skojarzonych z warstwą konwergencji, warstwa konwergencji jedynie
3843 wysyła i odbiera pakiety multicast. Pakietów unicast nie można wysłać. Jednakże, jest to wystarczające dla
3844 różnych protokołów wykrywania adresów do uzyskania adresu IPv6. Po zarejestrowaniu adresu IPv6
3845 warstwa IPv6 może przysyłać pakiety unicast, które mają adres źródłowy równy jednemu z jej
3846 zarejestrowanych adresów.

3847

3848 5.6.9.3.2 CL_IPv6_Register.request

3849 Ten prymityw jest przekazywany z warstwy IPv6 do warstwy konwergencji IPv6 do zarejestrowania adresu
3850 IPv6.

3851 Semantyka tego prymitywu przedstawia się następująco:

3852 CL_IPv6_REGISTER.request{ipv6, netmask, gateway}

3853 Adres IPv6 to adres do zarejestrowania.

3854 Maska sieciowa jest maską sieci wykorzystaną do maskowania numeru sieci z adresu. Maski podsieci
3855 używana jest przez warstwą konwergencji do określenia czy pakiet powinien być dostarczany bezpośrednio
3856 lub czy należy zastosować bramę.

3857 Adres IPv6 bramy, do której wysyłane mają zostać pakiety z adresem docelowym nie znajdującym się w tej
3858 samej podsieci co adres lokalny.

3859 Gdy adres IPv6 został zarejestrowany w węźle podstawowym, stosowany jest prymityw
3860 CL_IPv6_REGISTER.confirm. Jeśli rejestracja zakończy się niepowodzeniem, zastosowany zostanie prymityw
3861 CL_IPv6_RELEASE.confirm.

3862

3863 5.6.9.3.3 CL_IPv6_Register.confirm

3864 Ten prymityw jest przekazywany z warstwy konwergencji IPv6 do warstwy IPv6, aby wskazać, że rejestracja
3865 powiodła się.

3866 Semantyka tego prymitywu przedstawia się następująco:

3867 CL_IPv6_REGISTER.confirm{ipv6}

3868 Adres IPv6 to adres, który został zarejestrowany.

3869 Po zakończeniu rejestracji warstwa IPv6 może wysyłać pakiety IPv6 za pomocą adresu źródłowego.

3870

3871 **5.6.9.3.4 CL_IPv6_Unregister.request**

3872 Ten prymityw jest przekazywany z warstwy IPv6 do warstwy konwergencji IPv6 do wyrejestrowania adresu
3873 IPv6.

3874 Semantyka tego prymitywu przedstawia się następująco:

3875 `CL_IPv6_UNREGISTER.request{ipv6}`

3876 Adres IPv6 to adres do wyrejestrowania.

3877 Gdy adres IPv6 został wyrejestrowany z węzła podstawowego, stosowny jest prymityw
3878 CL_IPv6_UNREGISTER.confirm. Jeśli rejestracja zakończy się niepowodzeniem, zastosowany zostanie
3879 prymityw CL_IPv6_RELEASE.confirm.

3880

3881 **5.6.9.3.5 Unregister.confirm**

3882 Ten prymityw jest przekazywany z warstwy konwergencji IPv6 do warstwy IPv6, aby wskazać, że
3883 wyrejestrowanie powiodło się.

3884 Semantyka tego prymitywu przedstawia się następująco:

3885 `CL_IPv6_UNREGISTER.confirm{ipv6}`

3886 Adres IPv6 to adres, który został wyrejestrowany.

3887 Po zakończeniu wyrejestrowania warstwa IPv6 może wysyłać pakiety IPv6 za pomocą adresu źródłowego.

3888

3889 **5.6.9.4 Zarządzanie grupą multicast**

3890 **5.6.9.4.1 Ogólne**

3891 Ten rozdział opisuje prymitywy wykorzystywane do zarządzania grupami multicast.

3892 **5.6.9.4.2 CL_IPv6_MUL_Join.request**

3893 Ten prymityw jest przekazywany z warstwy IPv6 do warstwy konwergencji IPv6. Zawiera on adres multicast
3894 IPv6, do którego nastąpi dołączenie.

3895 Semantyka tego prymitywu przedstawia się następująco:

3896 `CL_IPv6_MUL_JOIN.request{IPv6 }`

3897 Adres IPv6 to grupa multicast IPv6, do której ma nastąpić dołączenie.

3898 Gdy warstwa konwergencji odbierze ten prymityw, będzie ona aranżować pakiety IPv6 wysyłane do tej
3899 grupy jako transmisje multicast w sieci PRIME i odbierać pakiety korzystające z tego adresu, które mają być
3900 przekazane do stosu IPv6. Jeśli podwarstwa konwergencji nie może dołączyć do grupy, korzysta ona z
3901 prymitywu CL_IPv6_MUL_LEAVE.confirm. W przeciwnym razie do wskazania powodzenia stosowany jest
3902 prymityw CL_IPv6_IGMP_JOIN.confirm.

3903 **5.6.9.4.3 CL_IPv6_MUL_Join.confirm**

3904 Ten prymityw jest przekazywany z warstwy konwergencji IPv6 do IPv6. Zawiera on status wyniku oraz adres
3905 multicast IPv6, do którego nastąpiło dołączenie.

3906 Semantyka tego prymitywu przedstawia się następująco:

3907 CL_IPv6_MUL_JOIN.confirm{IPv6}

3908 Adres IPv6 to grupa multicast IPv6, do której nastąpiło dołączenie. Warstwa konwergencji rozpocznie
3909 przekazywanie pakietów multicast IPv6 dla danej grupy multicast.

3910 **5.6.9.4.4 CL_IPv6_MUL_Leave.request**

3911 Ten prymityw jest przekazywany z warstwy IPv6 do warstwy konwergencji IPv6. Zawiera on adres multicast
3912 IPv6, który ma zostać opuszczony.

3913 Semantyka tego prymitywu przedstawia się następująco:

3914 CL_IPv6_MUL_LEAVE.request{IPv6}

3915 Adres IPv6 to grupa multicast IPv6, która będzie opuszczona. Warstwa konwergencji zakończy
3916 przekazywanie pakietów multicast IPv6 dla danej tej grupy i może opuścić grupę multicast MAC PRIME.

3917 **5.6.9.4.5 CL_IPv6_MUL_Leave.confirm**

3918 Ten prymityw jest przekazywany z warstwy konwergencji IPv6 do IPv6. Zawiera on status wyniku oraz adres
3919 multicast IPv6, który został opuszczony.

3920 Semantyka tego prymitywu przedstawia się następująco:

3921 CL_IPv6_MUL_LEAVE.confirm{IPv6, Result}

3922 Adres IPv6 to grupa multicast IPv6, która została opuszczona. Warstwa konwergencji zakończy
3923 przekazywanie pakietów multicast IPv6 dla danej grupy multicast.

3924 Parametr *Result* przyjmuje wartość z Tabela 134.

3925 Ten prymityw może być stosowany przez warstwę konwergencji jako wynik CL_IPv6_MUL_JOIN.request,
3926 CL_IPv6_MUL_LEAVE.request lub z powodu błędnego warunku prowadzącego do strat w połączeniu
3927 multicast PRIME MAC.

3928

3929 5.6.9.5 Transfer danych**3930 5.6.9.5.1 Ogólne**

3931 Poniższe prymitywy stosowane są do wysyłania i odbierania pakietów IPv6.

3932 5.6.9.5.2 CL_IPv6_DATA.request

3933 Ten prymityw jest przekazywany z warstwy IPv6 do warstwy konwergencji IPv6. Zawiera on jeden pakiet
3934 IPv6 do wysłania.

3935 Semantyka tego prymitywu przedstawia się następująco:

3936 CL_IPv6_DATA.request{IPv6_PDU}

3937 IPv6_PDU to pakiet IPv6 do wysłania.

3938 5.6.9.5.3 CL_IPv6_DATA.confirm

3939 Ten prymityw jest przekazywany z warstwy konwergencji IPv6 do warstwy IPv6. Zawiera on wskazanie
3940 statusu i pakiet IPv6, który właśnie został wysłany.

3941 Semantyka tego prymitywu przedstawia się następująco:

3942 CL_IPv6_DATA.confirm{IPv6_PDU, Result}

3943 IPv6_PDU to pakiet IPv6, który miał zostać wysłany.

3944 Wartość *Wyniku* wskazuje czy pakiet został wysłany, czy wystąpił błąd. Przyjmuje on wartość z Tabela 134.

3945 5.6.9.5.4 CL_IPv6_DATA.indicate

3946 Ten prymityw jest przekazywany z warstwy konwergencji IPv6 do warstwy IPv6. Zawiera on pakiet IPv6,
3947 który właśnie został odebrany.

3948 Semantyka tego prymitywu przedstawia się następująco:

3949 CL_IPv6_DATA.indicate{IPv6_PDU }

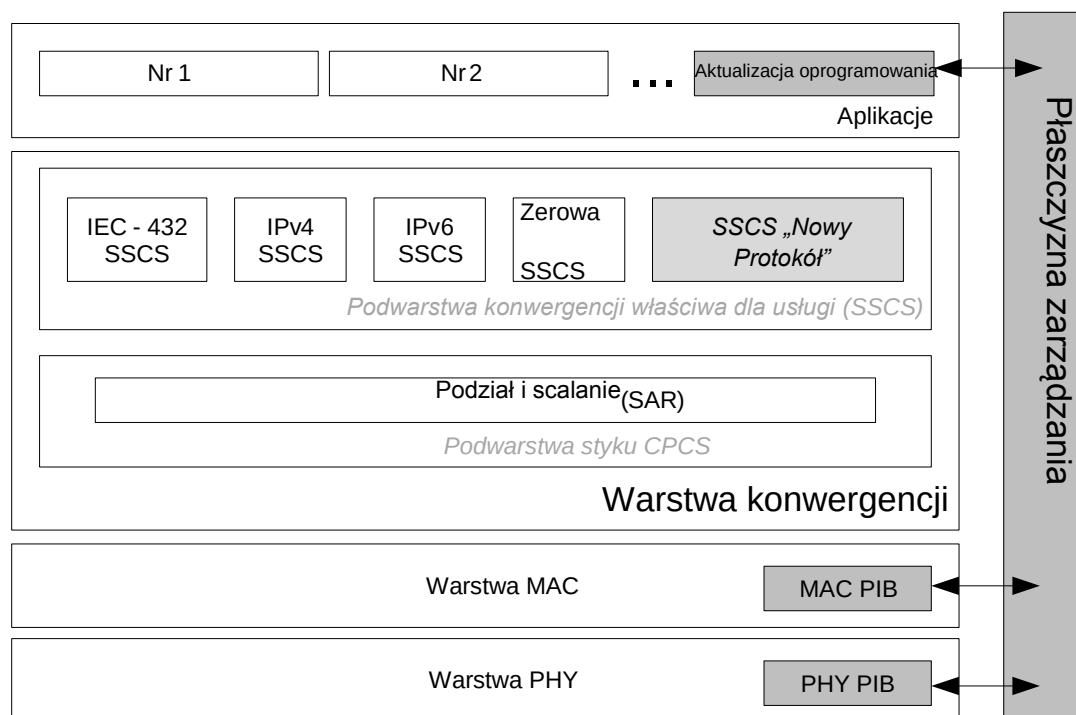
3950 IPv6_PDU to pakiet IPv6, który został odebrany.

3951

6 Płaszczyzna zarządzania

6.1 Wstęp

Ten rozdział opisuje funkcjonalność płaszczyzny zarządzania. Poniższy rysunek podkreśla położenie planu zarządzania w ogólnej architekturze protokołu.



Rys. 100 - Płaszczyzna zarządzania. Wprowadzenie.

Wszystkie węzły powinny wdrażać funkcjonalność płaszczyzn zarządzania opisaną w niniejszym punkcie. Płaszczyzna zarządzania umożliwia wykonywanie przez lokalną lub zdalną jednostkę kontrolną działań na węźle.

Obecna wersja tej specyfikacji wymienia funkcje płaszczyzny zarządzania do zarządzania węzłami i aktualizacją oprogramowania. Przyszłe wersje mogą zawierać dodatkowe funkcje zarządzania.

- Aby umożliwić dostęp do funkcji zarządzania w węźle serwisowym, węzeł podstawowy powinien otworzyć połączenie zarządzania po skutecznym ukończeniu rejestracji (patrz 6.4)
- Węzeł podstawowy może otworzyć takie połączenie albo natychmiast po udanej rejestracji lub jakiś czas później.
- Połączenie zarządzania unicast powinno zostać zidentyfikowane za pomocą CON.TYPE = TYPE_CL_MGMT.
- Istnieć mogą również połączenia zarządzania multicast. W czasie pisania tego dokumentu, połączenie zarządzania multicast stosowane jest wyłącznie do aktualizacji oprogramowania sprzętowego.
- Nie powinno być żadnych połączeń zarządzania broadcast.

- W przypadku, gdy węzeł serwisowy obsługuje połączenia ARQ, węzeł podstawowy powinien preferencyjnie spróbować otworzyć połączenie ARQ dla funkcji zarządzania.
- Funkcje płaszczyzny zarządzania powinny korzystać z zerowej SSCS jak określono w punkcie 5.3

6.2 Zarządzanie węzłami

6.2.1 Ogólne

Zarządzanie węzłami odbywa się za pomocą zestawu atrybutów. Atrybuty zdefiniowane są zarówno dla warstwy PHY jak i warstwy MAC. Zestaw tych atrybutów zarządzania nazywa się Bazą informacji PLC (PIB). Niektóre atrybuty są tylko do odczytu, podczas gdy inne są do odczytu i do zapisu.

Identyfikatory atrybutu PIB mają wartość 16-bitową. Pozwala to na określenie do 65535 atrybutów PIB.

- Wartości identyfikatora atrybutu PIB od 0 do 32767 są otwarte na standaryzację. Żadne zastrzeżone atrybuty nie mogą mieć identyfikatorów w tym zakresie.
- Wartości w zakresie 32768 do 65535 są otwarte dla określonych zastosowań dostawców.

Identyfikatory atrybutów PIB w standardowym zakresie (0 do 32767), które nie są określone w tej wersji specyfikacji są zastrzeżone dla wykorzystania w przyszłości.

Uwaga: Tabela atrybutów PIB poniżej wskazuje typ każdego atrybutu. Dla typów liczb całkowitych wielkość liczby całkowitej została określony w bitach. Wdrożenie może korzystać z większej liczby całkowitej dla atrybutu, jednak nie wolno używać mniejszego rozmiaru.

6.2.2 Atrybuty PIB warstwy PHY

6.2.2.1 Ogólne

Realizacja warstwy PHY w każdym urządzeniu może opcjonalnie zarządzać zbiorem atrybutów, które zawierają szczegółowe informacje na temat jej pracy. Atrybuty warstwy PHY stanowią część bazy informacji PLC (PIB).

6.2.2.2 Atrybuty statystyczne

Warstwa fizyczna dostarcza informacje statystyczne dla celów zarządzania. Kolejna tabela podaje statystyki udostępniane przez warstwę PHY jednostkom zarządzającym przez prymityw PLME_GET. Pole ID w tej tabeli jest parametrem usługi prymitywu PLME_GET opisanego w punkcie 3.10.4.

Tabela 90 - Zmienne tylko do odczytu warstwy PHY dostarczające informacje statystyczne

Nazwa atrybutu	Rozmiar (w bitach)	ID	Opis
phyStatsCRCIncorrectCount	16	0x00A0	Liczba transmisji seryjnych odebrana na warstwie PHY, dla której kontrola CRC nie powiodła się.
phyStatsCRCFailCount	16	0x00A1	Liczba transmisji seryjnych odebrana na warstwie

			PHY, dla której kontrola CRC powiodła się, ale pole <i>Protocol</i> w nagłówku PHY miało nieprawidłową wartość. Ta liczba będzie odzwierciedlać liczbę razy uszkodzone dane zostały odebrane, a kontrola CRC nie wykryła tego.
phyStatsTxDropCount	16	0x00A2	Liczba razy, gdy warstwa PHY odebrała nowe dane do przesłania (PHY_DATA.request) i musiała albo nadpisać istniejące dane w kolejce transmisji lub zrzucić dane do nowego żądania z powodu pełnej kolejki.
phyStatsRxDropCount	16	0x00A3	Liczba razy, gdy warstwa PHY odebrała nowe dane na kanale i musiała albo nadpisać istniejące dane w kolejce odbierania lub zrzucić nowo odebrane dane z powodu pełnej kolejki.
phyStatsRxTotalCount	32	0x00A4	Łączna liczba prawidłowo rozszyfrowanych jednostek PPDU. Przydatna dla przypadków testowania warstwy PHY do oszacowania FER.
phyStatsBlkAvgEvm	16	0x00A5	Wykładnicza średnia krocząca EVM w ostatnich 16 jednostkach PPDU, w stanie zwróconym przez prymityw PHY_SNR. Należy pamiętać, że prymityw PHY_SNR zwraca 3-bitową liczbę w skali dB. Więc pierwsza 3-bitowa liczba dB konwertowana jest na skalę liniową (liczba k przechodzi w $2^{(k/2)}$), uzyskując 7-bitową liczbę z 3 bitami ułamkowymi. Wynik gromadzony jest w 16 PPDU i zgłaszany.
phyEmaSmoothing	8	0x00A8	Dzielnik współczynnika wygładzania dla wartości, które są aktualizowane jako wykładnicza średnia krocząca. Kolejna wartość to: $V_{next} = S * NewSample + (1 - S) * V_{prev}$ Gdzie $S = 1 / (2^{phyEMASmoothing})$

4000 6.2.2.3 Wdrażanie atrybutów

4001 Możliwe jest wdrożenie funkcji PHY zgodnych z tą specyfikacją na wiele sposobów. Wiele opcji
 4002 wdrożeniowych zapewnia pewien stopień nieprzewidywalności dla warstw MAC. Implementacje PHY mogą
 4003 ewentualnie dostarczyć szczegółowych informacji na temat parametrów, które są przedmiotem
 4004 zainteresowania warstwy MAC za pośrednictwem prymitywu PLME_GET. Wykaz takich parametrów, dla

4005 których zapytania mogą być składane przez MAC w zakresie prymitywów PLME_GET można znaleźć w
 4006 Tabela 91 - Wszystkie atrybuty podane w Tabela 91 - są stałymi implementacyjnymi i nie można ich
 4007 zmieniać.

4008 **Tabela 91 - Parametry tylko do odczytu warstwy PHY dostarczające informacje na temat określonego wdrożenia**

Nazwa atrybutu	Rozmiar (w bitach)	ID	Opis
phyTxQueueLen	10	0x00B0	Liczba jednoczesnych MPDU, które mogą pomieścić bufor transmitujący warstwy PHY.
phyRxQueueLen	10	0x00B1	Liczba jednoczesnych MPDU, które mogą pomieścić bufor odbierający warstwy PHY.
phyTxProcessingDelay	20	0x00B2	Czas, jaki upłynął od wystąpienia odebrania danych w interfejsie komunikacyjnym MAC-PHY do momentu, gdy znajdują się one w kanale fizycznym. Nie powinien on obejmować opóźnień w komunikacji przez interfejs MAC-PHY. Wartość atrybutu podana jest w mikrosekundach.
phyRxProcessingDelay	20	0x00B3	Czas, jaki upłynął od wystąpienia odebrania danych w kanale fizycznym do momentu, gdy dane zostaną udostępnione MAC w interfejsie komunikacyjnym MAC-PHY. Nie powinien on obejmować opóźnień w komunikacji przez interfejs MAC-PHY. Wartość atrybutu podana jest w mikrosekundach.
phyAgcMinGain	8	0x00B4	Minimalne wzmocnienie dla AGC ≤ 0 dB.
phyAgcStepValue	3	0x00B5	Odległość pomiędzy krokami w dB ≤ 6 dB.
phyAgcStepNumber	8	0x00B6	Liczba kroków, tak że $\text{phyAgcMinGain} + (\text{phyAgcStepNumber} - 1) * \text{phyAgcStepValue} \geq 21$ dB.

4009

4010 6.2.3 Atrybuty PIB MAC

4011 6.2.3.1 Ogólne

4012 **Uwaga:** Należy zauważyć, że kolumna „O” (Obowiązkowe) w tabelach poniżej oznacza czy atrybuty PIB są
 4013 obowiązkowe dla wszystkich urządzeń (zarówno węzły serwisowe jak i podstawowe określone jako
 4014 „Wszystkie”), tylko dla węzłów serwisowych („SN”), tylko dla węzłów podstawowych („BN”) lub w ogóle nie
 4015 są obowiązkowe („Nie”).

6.2.3.2 Zmienne atrybuty MAC

Zmienne PIB MAC obejmują zestaw atrybutów PIB, które wpływają na zachowanie funkcjonalne implementacji. Te atrybuty mogą być zdefiniowane zewnętrznie do MAC, zazwyczaj przez jednostkę zarządzającą, a wdrożenia mogą dopuszczać zmiany w ich wartościach w czasie normalnej pracy, tj. nawet po wykonaniu sekwencji uruchomienia urządzenia.

Zewnętrzna jednostka zarządzająca może mieć dostęp do tych atrybutów poprzez zestaw prymitywów MLME_GET (4.5.5.7) i MLME_SET (4.5.5.9). Pole ID w tabeli poniżej będzie atrybutem *PIBAttribute*, który należy przekazać do punktu dostępu MLME podczas pracy na tych atrybutach.

Tabela 92 - Tablica zmiennych do odczytu/zapisu warstwy MAC

Nazwa atrybutu	ID	Typ	O	Prawidłowy zakres	Opis	Def.
macMinSwitchSearchTime	0x0010	Integer8	Nie	16 – 32 sekund	Minimalny czas, przez który węzeł serwisowy w stanie <i>Rozłączony</i> powinien skanować kanał pod kątem sygnałów przed wysłaniem PNPDU. Atrybut ten nie jest zarządzany w węzłach podstawowych.	24
macMaxPromotionPdu	0x0011	Integer8	Nie	1 – 4	Maksymalna liczba jednostek PNPDU, jaką można przestać w okresie <i>macPromotionPduTxPeriod</i> sekund. Atrybut ten nie jest zarządzany w węźle podstawowym.	2
macPromotionPduTxPeriod	0x0012	Integer8	Nie	2 – 8 sekund	Kwant czasu do ograniczania liczby jednostek PNPDU przesyłanych z węzła serwisowego. W okresie <i>macPromotionPduTxPeriod</i> sekund nie można przestać więcej niż <i>macMaxPromotionPdu</i> .	5

Nazwa atrybutu	ID	Typ	O	Prawidłowy zakres	Opis	Def.
macBeaconsPerFrame	0x0013	Integer8	BN	1 – 5	Maksymalna liczba szczelin sygnału, które mogą być dostarczone w ramce. Atrybut ten jest zarządzany w węźle podstawowym.	5
macSCPMaTxAttempts	0x0014	Integer8	Nie	2 – 5	Liczba razy, ile algorytm CSMA będzie próbować przestać żądane dane, podczas gdy poprzednia próba została wstrzymana w wyniku wskazania zajętości kanału przez warstwę PHY.	5
macCtlReTxTimer	0x0015	Integer8	Nie	2 – 20 sekund	Liczba sekund, przez którą jednostka MAC czeka na zatwierdzenie odebrania pakietu kontrolnego MAC z jednostki równorzędnej. Po zakończeniu tego okresu jednostka MAC może ponownie transmitować pakiet kontrolny MAC.	15
macMaxCtlReTx	0x0018	Integer8	Nie	3 – 5	Maksymalna liczba razy, gdy jednostka MAC spróbuje retransmisji niepotwierdzonych pakietów kontrolnych MAC. Jeśli liczba retransmisji osiągnie maksymalną wartość, jednostka MAC zaprzestanie dalszych prób wysłania pakietu kontrolnego MAC.	3
macEMASmoothing	0x0019	Integer8	Wsyztkie	0 - 7	Dzielnik współczynnika wygładzania dla wartości, które są aktualizowane jako wykładnicza średnia krocząca. Kolejna wartość to:	3

Nazwa atrybutu	ID	Typ	O	Prawidłowy zakres	Opis	Def.
					$V_{next} = S * NewSample + (1 - S) * V_{prev}$ Gdzie $S = 1 / (2^{macEMASmoothing})$.	

4025

4026

Tabela 93 - Tablica zmiennych tylko do odczytu warstwy MAC

Nazwa atrybutu	ID	Typ	O	Prawidłowy zakres	Opis	Def.
macSCPRBO	0x0016	Integer8	Nie	1 – 15 symboli	Losowy okres oczekiwania, dla którego realizacja powinna opóźnić start iteracji wykrywania kanału podczas prób przesyłania danych w okresie współdzielonej kontencji. Jest to atrybut „tylko do odczytu”.	-
macSCPChSenseCount	0x0017	Integer8	Nie	2 – 5	Liczba razy, kiedy wdrożenie musi wykonać proces wykrywania kanału. Jest to atrybut „tylko do odczytu”.	-

4027

6.2.3.3 Atrybuty funkcjonalne

4028

4029

4030

4031

Niektóre atrybuty PIB należą do zachowania funkcjonalnego MAC. Dostarczają one informacji na temat określonych aspektów. Jednostka zarządzająca może jedynie odczytywać aktualne wartości za pomocą prymitywów MLME_GET. Wartości tych atrybutów nie mogą być zmienione przez jednostkę zarządzania poprzez prymitywy MLME_SET.

4032

4033

Pole ID w tabeli poniżej będzie atrybutem *PIBAttribute*, który należy przekazać do punktu dostępu MLME_GET w celu uzyskania dostępu do wartości tych atrybutów.

4034

Tabela 94 - Tablica zmiennych tylko do odczytu warstwy MAC, które dostarczają informacje funkcjonalne

Nazwa atrybutu	ID	Typ	O	Prawidłowy zakres	Opis

Nazwa atrybutu	ID	Typ	O	Prawi dłowy zakres	Opis
macLNID	0x0020	Integer16	SN	0 – 16383	LNID przypisany do tego węzła w czasie jego rejestracji.
MacLSID	0x0021	Integer8	SN	0 – 255	LNID przydzielony do tego węzła w czasie jego promocji. Atrybut ten nie jest zarządzany jeśli węzeł znajduje się w stanie funkcjonalnym <i>Terminal</i> .
MacSID	0x0022	Integer8	SN	0 – 255	Identyfikator SID węzła przełączającego, przez który ten węzeł połączony jest z podsiecią. Atrybut ten nie jest zarządzany w węźle podstawowym.
MacSNA	0x0023	EUI-48	SN		Adres podsieci, w której zarejestrowany jest węzeł. Węzeł podstawowy zwraca SNA, z którego korzysta.
MacState	0x0024	Wyliczenie	SN		Aktualny stan funkcjonalny węzła.
				0	ROZŁĄCZONY.
				1	TERMINAL.
				2	PRZEŁĄCZENIE.
				3	PODSTAWA.
MacSCPLength	0x0025	Integer16	SN		Długość SCP w symbolach, w aktualnej ramce.
MacNodeHierarchyLevel	0x0026	Integer8	SN	0 – 63	Poziom tego węzła w hierarchii podsieci.
MacBeaconSlotCount	0x0027	Integer8	SN	0 – 7	Liczba szczelin sygnału przewidziana w aktualnej strukturze ramki.

Nazwa atrybutu	ID	Typ	O	Prawi dłowy zakres	Opis
macBeaconRxSlot	0x0028	Integer8	SN	0 – 7	Szczelina sygnału, w której węzeł przełączający urządzenia transmituje swój sygnał. Atrybut ten nie jest zarządzany w węźle podstawowym.
MacBeaconTxSlot	0x0029	Integer8	SN	0 – 7	Szczelina sygnału, w której to urządzenie transmituje swój sygnał. Atrybut ten nie jest zarządzany w węzłach serwisowych znajdujących się w stanie funkcjonalnym <i>Terminal</i> .
MacBeaconRxFrequency	0x002A	Integer8	SN	0 – 31	Liczba ramek pomiędzy odbiorami dwóch skutecznych sygnałów. Wartość 0x0 wskazuje, że sygnały są odbierane w każdej ramce. Atrybut ten nie jest zarządzany w węźle podstawowym.
MacBeaconTxFrequency	0x002B	Integer8	SN	0 – 31	Liczba ramek pomiędzy transmisjami dwóch skutecznych sygnałów. Wartość 0x0 wskazuje, że sygnały są wysyłane w każdej ramce. Atrybut ten nie jest zarządzany w węzłach serwisowych znajdujących się w stanie funkcjonalnym <i>Terminal</i> .

Nazwa atrybutu	ID	Typ	O	Prawi dłowy zakres	Opis
MacCapabilities	0x002C	Integer16	Ws zys tki e	Mapa bitowa	Mapa bitowa uprawnień MAC danego urządzenia. Ten atrybut będzie zarządzany na wszystkich urządzeniach. Bity w ciągu od prawej do lewej mają następujące znaczenie: Bit0: Możliwe przełączenie; Bit1: Agregacja pakietów; Bit2: Okres bezkolizyjnego dostępu; Bit3: Połączenie bezpośrednie; Bit4: Multicast; Bit5: Zarządzanie stabilnością PHY; Bit6: ARQ; Bit7: Zarezerwowany do użytku w przyszłości. Bit8: Przełączenie połączenia bezpośredniego; Bit9: Przełączenie multicast możliwe; Bit10: Możliwość zarządzania odpornością warstwy PHY; Bit11: Przełączanie buforowania ARQ możliwe; Bity 12 do 15: Zarezerwowany do użytku w przyszłości.

4035 6.2.3.4 Atrybuty statystyczne

4036 Warstwa MAC dostarcza informacje statystyczne dla celów zarządzania. Tabela 95 podaje statystyki
4037 udostępniane przez MAC jednostkom zarządzającym przez prymityw MLME_GET.

4038 Pole ID w tabeli poniżej będzie atrybutem *PIBAttribute*, który należy przekazać do punktu dostępu
4039 MLME_GET w celu uzyskania dostępu do wartości tych atrybutów.

4040

Tabela 95 - Tablica zmiennych tylko do odczytu warstwy MAC, które dostarczają informacje statystyczne

Nazwa atrybutu	ID	O	Typ	Opis
macTxDataPktCount	0x0040	Nie	Integer32	Liczba pomyślnie przesłanych MSDU.
MacRxDataPktCount	0x0041	Nie	Integer32	Liczba pomyślnie odebranych jednostek MSDU, których adres docelowy był tym węzłem.
MacTxCtrlPktCount	0x0042	Nie	Integer32	Liczba pomyślnie przesłanych pakietów kontrolnych MSDU.
MacRxCtrlPktCount	0x0043	Nie	Integer32	Liczba pomyślnie odebranych pakietów kontrolnych MAC, których adres docelowy był tym węzłem.
MacCSMAFailCount	0x0044	Nie	Integer32	Liczba nieudanych prób przesyłania CSMA.
MacCSMAChBusyCount	0x0045	Nie	Integer32	Liczba razy ten węzeł musiał wycofać transmisję SCP z powodu stanu zajętości kanału.

4041

6.2.3.5 Atrybuty listy MAC

4042

Warstwa MAC sporządza pewne listy dostępne dla jednostek zarządzających przez prymityw

4043

MLME_LIST_GET. Listy te podano w Tabeli 96. Mimo że jednostka zarządzająca może odczytać każdą z tych

4044

list, nie może zmienić treści żadnej z nich.

4045

Pole ID w tabeli poniżej będzie atrybutem *PIBListAttribute*, który należy przekazać do punktu dostępu

4046

MLME_LIST_GET w celu uzyskania dostępu do wartości tych atrybutów.

4047

Tabela 96 - Tablica listy tylko do odczytu udostępnianych przez warstwę MAC przez interfejs zarządzania

Nazwa atrybutu listy	ID	O	Opis		
macListRegDevices	0x0050	BN	Lista zarejestrowanych urządzeń. Lista ta zarządzana jest wyłącznie przez węzeł podstawowy. Każda pozycja na liście składa się z następujących informacji.		
			Element wejściowy	Typ	Opis
			regEntryID	EUI-48	EUI-48 zarejestrowanego węzła.
			regEntryLNID	Integer16	LNID przydzielony do tego węzła.

Nazwa listy	atrybutu	ID	O	Opis		
				regEntryState	TERMINAL=1 , PRZEŁĄCZANIE=2	Stan funkcjonalny tego węzła.
				regEntryLSID	Integer16	SID przydzielony do tego węzła.
				regEntrySID	Integer16	Identyfikator przełączenia, przez które połączony jest ten węzeł.
				regEntryLevel	Integer8	Poziom hierarchii tego węzła.
				regEntryTCap	Integer8	Mapa bitowa uprawnień MAC funkcji Terminala w tym urządzeniu. Bity w ciągu od prawej do lewej mają następujące znaczenie: - Bit0: Możliwe przełączenie; - Bit1: Agregacja pakietów; - Bit2: Okres bezkolizyjnego dostępu; - Bit3: Połączenie bezpośrednie; - Bit4: Multicast; - Bit5: Zarządzanie stabilnością PHY; - Bit6: ARQ; - Bit7: Zarezerwowany do użytku w przyszłości.

Nazwa atrybutu listy	ID	O	Opis		
			regEntrySwCap	Integer8	Mapa bitowa uprawnień do przełączania MAC tego urządzenia. Bity w ciągu od prawej do lewej mają następujące znaczenie: Bit0: Przełączenie połączenia bezpośredniego możliwe; Bit1: Przełączenie multicast; Bit2: Możliwość zarządzania odpornością warstwy PHY; Bit3: Przełączanie buforowania ARQ możliwe; Bit4 do 7: Zarezerwowany do użytku w przyszłości.
macListActiveConn	0x0051	BN	Lista aktywnych połączeń niebezpośrednich. Lista ta zarządzana jest wyłącznie przez węzeł podstawowy.		
			Element wejściowy	Typ	Opis
			connEntrySID	Integer16	Identyfikator przełączenia, przez które połączony jest węzeł serwisowy.
			connEntryLNID	Integer16	Identyfikator węzła przypisany do węzła serwisowego.
			connEntryLCID	Integer8	Identyfikator połączenia lokalnego przypisanego do tego połączenia.
			connEntryID	EUI-48	EUI-48 węzła serwisowego.
macListMcastEntries	0x0052	Nie	Lista pozycji w tablicy przełączania multicast. Lista ta nie jest zarządzana przez węzły serwisowe w stanie funkcjonalnym <i>Terminal</i> .		

Nazwa listy	atrybutu	ID	O	Opis		
				Element wejściowy	Typ	Opis
				mcastEntryLCID	Integer8	LCID grupy multicast.
				mcastEntryMembers	Integer16	Liczba węzłów potomków (w tym samego węzła), które są członkami tej grupy.
macListSwitchTable	0x0053	SN	Lista tablic przełączania. Lista ta nie jest zarządzana przez węzły serwisowe w stanie funkcjonalnym <i>Terminal</i> .			
			Element wejściowy	Typ	Opis	
			stblEntryLSID	Integer16	SID przyłączonego węzła serwisowego.	
macListDirectConn	0x0054	Nie	Lista aktywnych połączeń bezpośrednich. Lista zarządzana jest wyłącznie w węźle podstawowym.			
			Element wejściowy	Typ	Opis	
			dconnEntrySrcSID	Integer16	Identyfikator przełączenia przez które połączony jest źródłowy węzeł serwisowy.	
			dconEntrySrcLNID	Integer16	Identyfikator węzła przypisany do źródłowego węzła serwisowego.	
			dconnEntrySrcLCID	Integer8	Identyfikator połączenia lokalnego przypisanego do tego połączenia u źródła.	
			dconnEntrySrcID	EUI-48	EUI-48 źródłowego węzła docelowego.	
			dconnEntryDstSID	Integer16	Identyfikator przełączenia, przez które połączony jest docelowy węzeł serwisowy.	

Nazwa listy	atrybutu	ID	O	Opis		
				dconnEntryDstLNID	Integer16	Identyfikator węzła przypisany do docelowego węzła serwisowego.
				dconnEntryDstLCID	Integer8	Identyfikator połączenia lokalnego przypisanego do tego połączenia w lokalizacji docelowej.
				dconnEntryDstID	EUI-48	EUI-48 docelowego węzła serwisowego.
				dconnEntryDSID	Integer16	SID przełączenia, które jest przełączeniem bezpośrednim.
				dconnEntryDID	EUI-48	EUI-48 przełączenia bezpośredniego.
macListDirectTable	0x0055	Nie	Lista tablic przełączania bezpośredniego			
			Element wejściowy	Typ	Opis	
			dconnEntrySrcSID	Integer16	Identyfikator przełączenia przez które połączony jest źródłowy węzeł serwisowy.	
			dconnEntrySrcLNID	Integer16	Identyfikator węzła przypisany do źródłowego węzła serwisowego.	
			dconnEntrySrcLCID	Integer8	Identyfikator połączenia lokalnego przypisanego do tego połączenia u źródła.	
			dconnEntryDstSID	Integer16	Identyfikator przełączenia, przez które połączony jest docelowy węzeł serwisowy.	
			dconnEntryDstLNID	Integer16	Identyfikator węzła przypisany do docelowego węzła serwisowego.	

Nazwa atrybutu listy	ID	O	Opis		
			dconnEntryDstLCID	Integer8	Identyfikator połączenia lokalnego przypisanego do tego połączenia w lokalizacji docelowej.
			dconnEntryDID	EUI-48	EUI-48 przełączenia bezpośredniego.
macListAvailableSwitches	0x0056	SN	Wykaz węzłów przełączających, których sygnały zostały odebrane.		
			Element wejściowy	Typ	Opis
			slistEntrySNA	EUI-48	EUI-48 podsieci.
			slistEntryLSID	Integer16	SID tego przełączenia.
			slistEntryLevel	Integer8	Poziom tego przełączenia w hierarchii podsieci.
			slistEntryRxLvl	Integer8 EMA	Poziom odebranego sygnału dla tego przełączenia.
			slistEntryRxSNR	Integer8 EMA	Stosunek sygnału do szumu dla tego przełączenia.
macListPhyComm	0x0057	Wszystkie	Lista parametrów komunikacji warstwy PHY. Tablica zarządzana jest w każdym węźle. Dla węzłów terminala zawiera ona jedną pozycję dla przełączenia, do którego podłączony jest węzeł. Dla innych węzłów zawiera ona również pozycje dla każdego bezpośrednio podłączonego węzła potomka (child node).		
			Element wejściowy	Typ	Opis
			phyCommEUI	EUI-48	EUI-48 innego urządzenia.
			phyCommTxPwr	Integer8	Moc Tx pakietów GPDU wysyłanych do urządzenia.

Nazwa atrybutu listy	ID	O	Opis		
			phyCommTxCod	Integer8	Kodowanie Tx pakietów GPDU wysyłanych do urządzenia.
			phyCommRxCod	Integer8	Kodowanie Rx pakietów GPDU odebranych z urządzenia.
			phyCommRxLvl	Integer8 EMA	Poziom mocy Rx pakietów GPDU odebranych z urządzenia.
			phyCommSNR	Integer8 EMA	Stosunek sygnału do szumu pakietów GPDU odebranych z urządzenia.
			phyCommTxPwrMod	Integer8	Ilość razy moc Tx była modyfikowana.
			phyCommTxCodMod	Integer8	Ilość razy kodowanie Tx było modyfikowane.
			phyCommRxCodMod	Integer8	Ilość razy kodowanie Rx było modyfikowane.

4048 6.2.3.6 Atrybuty PIB działania

4049 Niektóre testy zgodności wymagają uruchomienia pewnych działań na węzłach serwisowych. Poniższa
 4050 tabela podaje zestaw atrybutów działań, które muszą być obsługiwane przez wszystkie implementacje.

4051 Tabela 97 - Atrybuty PIB działania

Nazwa atrybutu	ID	O	Rozmiar (w bitach)	Opis
MACActionTxData	0x0060	SN	8	Łączna liczba prawidłowo rozszyfrowanych jednostek PPDU. Przydatna dla warstwy PHY do oszacowania FER.
MACActionConnClose	0x0061	SN	8	Wyzwolenie do zamknięcia jednego z otwartych połączeń.
MACActionRegReject	0x0062	SN	8	Wyzwolenie odrzucenia żądania rejestracji

Nazwa atrybutu	ID	O	Rozmiar (w bitach)	Opis
				przychodzącej.
MACActionProReject	0x0063	SN	8	Wyzwolenie odrzucenia żądania promocji przychodzącej.
MACActionUnregister	0x0064	SN	8	Wyzwolenie wyrejestrowania z podsieci.

4052 6.2.4 Atrybuty PIB aplikacji

4053 Poniższe atrybuty PIB są wykorzystywane do ogólnego zarządzania urządzeniami zgodnymi z OFDM PRIME.
 4054 Atrybuty te i klucz SWK nie wpływają na funkcjonalność komunikacji, ale umożliwiają łatwiejsze
 4055 zarządzanie.

4056 Atrybuty te powinny być obsługiwane zarówno przez urządzenia węzła podstawowego i węzła
 4057 serwisowego.

4058 Tabela 98 - Atrybuty PIB aplikacji

Nazwa atrybutu	Rozmiar (w bitach)	ID	Opis
AppFwVersion	128	0x0075	Opis tekstowy wersji oprogramowania działającego na urządzeniu.
AppVendorId	16	0x0076	Przypisany unikalny identyfikator dostawcy PRIME Alliance.
AppProductId	16	0x0077	Przypisany unikalny identyfikator dostawcy dla określonego produktu.

4059 6.3 Aktualizacja oprogramowania sprzętowego

4060 6.3.1 Ogólne

4061 Niniejszy punkt opisuje aktualizację oprogramowania sprzętowego. Urządzenia obsługujące OFDM PRIME
 4062 mogą mieć zainstalowane kilka typów oprogramowania sprzętowego, co najmniej jeden, który obsługuje
 4063 samą aplikację oraz jeden powiązany z protokołem OFDM PRIME. Mimo że jest możliwe, aby aplikacja
 4064 mogła przeprowadzać aktualizację oprogramowania sprzętowego wszystkich obrazów oprogramowania
 4065 sprzętowego urządzenia, na przykład transfer obrazu DLMS/COSEM za pomocą obiektu przesyłającego
 4066 obraz COSEM, obsługa aktualizacji oprogramowania sprzętowego OFDM PRIME jest obowiązkowa w celu
 4067 przetworzenia aktualizacji oprogramowania sprzętowego OFDM PRIME niezależnie od aplikacji.

4068 6.3.2 Wymagania i funkcje

4069 Ten punkt opisuje aplikację do aktualizacji oprogramowania, która jest unikalna i obowiązkowa dla węzłów
4070 podstawowych i serwisowych.

4071 Najważniejsze cechy mechanizmu aktualizacji oprogramowania sprzętowego podano poniżej. Aby uzyskać
4072 więcej informacji, patrz kolejne punkty. Mechanizm oprogramowania sprzętowego:

- 4073 • Powinien stanowić część płaszczyzny zarządzania, a zatem korzystać z zerowej SSCS jak określono w
4074 punkcie 5.3
- 4075 • Może pracować w unicast (tryb domyślny) i multicast (tryb opcjonalny). Komunikaty kontrolne
4076 zawsze są wysyłane za pomocą połączeń unicast, podczas gdy dane mogą być przesyłane za pomocą
4077 zarówno unicast i multicast. Do przesyłania danych nie należy stosować broadcast.
- 4078 • Może zmieniać rozmiary pakietów danych zgodnie z warunkami kanału. Rozmiar pakietu nie
4079 zostanie zmieniony w czasie procesu pobierania.
- 4080 • Jest w stanie w dowolnym momencie wysłać do węzłów serwisowych żądanie o przekazanie
4081 podstawowych informacji, takich jak model urządzenia, wersja oprogramowania i wersja protokołu
4082 aktualizacji oprogramowania.
- 4083 • Przerwanie jego wykonywania powinno być możliwe w dowolnym momencie.
- 4084 • Sprawdza poprawność pobranego oprogramowania sprzętowego po zakończeniu odbierania. W
4085 przypadku niepowodzenia aplikacja aktualizująca oprogramowanie sprzętowe powinna zażądać
4086 nowej retransmisji.
- 4087 • Nowe oprogramowanie sprzętowe powinno być wykonywane w węzłach podstawowych jedynie jeśli
4088 mają one nakaz, by to zrobić. Aplikacja aktualizacji oprogramowania powinna być w stanie ustawić
4089 moment, w którym nastąpi resetowanie.
- 4090 • Musi być w stanie odrzucić nowe oprogramowanie po okresie „testowym” i przełączać się na starą
4091 wersję. Czas trwania tego okresu próbnego musi być ustalany przez mechanizm aktualizacji
4092 oprogramowania sprzętowego.

4093 6.3.3 Opis ogólny

4094 6.3.3.1 Ogólne

4095 Mechanizm aktualizacji oprogramowania sprzętowego jest w stanie pracować w trybach unicast i multicast.
4096 Wszystkie komunikaty kontrolne są wysyłane za pomocą połączeń unicast, podczas gdy dane mogą być
4097 wysyłane za pośrednictwem unicast (domyślnie) lub multicast (tylko jeśli jest obsługiwane przez
4098 producenta). Należy zauważyć, że aby zapewnić poprawny odbiór oprogramowania sprzętowego podczas
4099 aktualizacji węzłów serwisowych różnych dostawców, pakiety danych nie powinny być wysyłane za
4100 pośrednictwem transmisji broadcast. Dopuszczalne są tylko unicast i multicast. Węzeł odpowie wyłącznie
4101 na komunikaty wysyłane za pośrednictwem unicast. Patrz punkt 6.3.5, aby uzyskać szczegółowy opis
4102 komunikatów kontrolnych i informacyjnych stosowanych przez mechanizm aktualizacji oprogramowania
4103 sprzętowego.

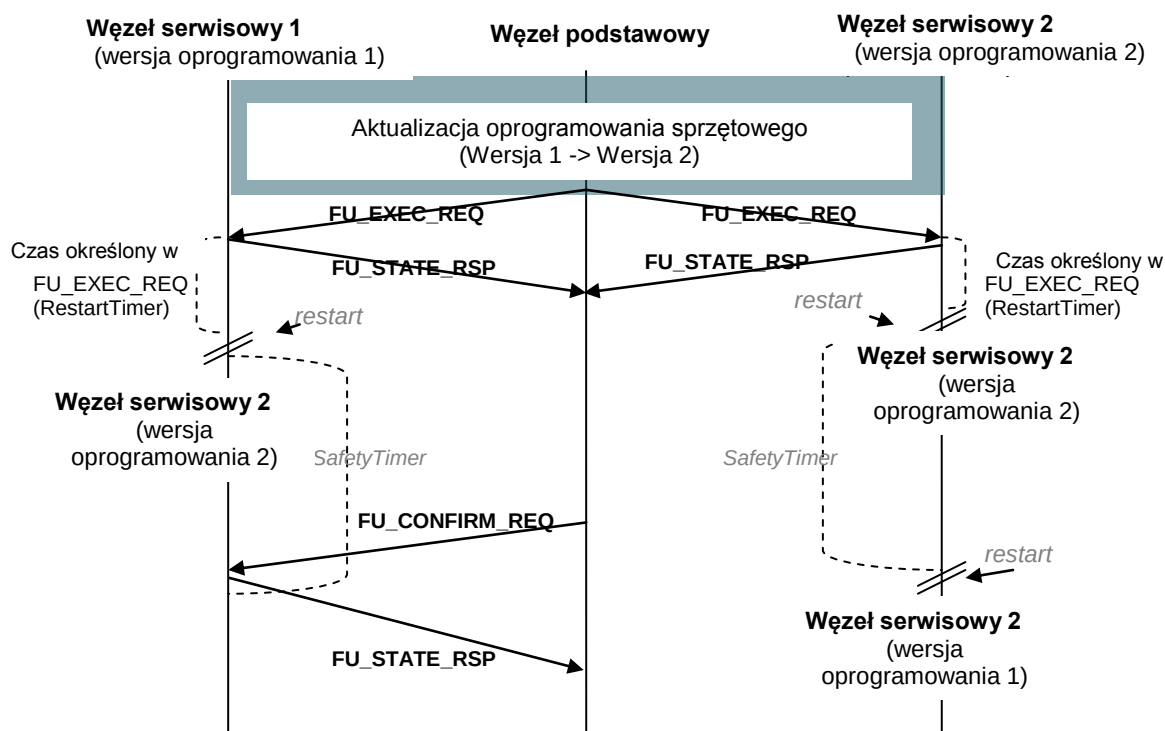
4104 Połączenia unicast i multicast są ustanawiane przez węzeł podstawowy. W przypadku obsługi multicast
4105 węzeł podstawowy powinien zażądać od węzłów określonych dostawców dołączenia do określonej grupy
4106 multicast, która została wyłącznie utworzona do przeprowadzenia aktualizacji oprogramowania
4107 sprzętowego i zostaje usunięta po zakończeniu jej.

4108 Jak powiedziano wcześniej, od dostawcy zależy stosowanie unicast lub multicast do przesyłania danych. W
4109 przypadku transmisji danych unicast należy zauważyć, że zastosowanie ARQ jest funkcją opcjonalną.
4110 Przykłady pokazujące ruch pomiędzy węzłem podstawowym a węzłami serwisowymi w unicast i multicast
4111 pokazano w punkcie 6.3.6.

4112 Po ukończeniu pobierania oprogramowania sprzętowego węzeł podstawowy nakazuje każdemu węzłowi
4113 serwisowemu sprawdzenie integralności danych. Pobieranie oprogramowania sprzętowego zostanie
4114 ponownie uruchomione, jeśli obraz oprogramowania sprzętowego będzie uszkodzony. W innym przypadku
4115 węzły serwisowe będą czekać do czasu, gdy węzeł podstawowy nakaże im uruchomienie nowego
4116 oprogramowania sprzętowego.

4117 Mechanizm aktualizacji oprogramowania sprzętowego może skonfigurować wystąpienie, gdy niedawno
4118 pobrane oprogramowanie wykonywane jest w węzłach serwisowych. W ten sposób węzeł podstawowy
4119 może ponownie uruchomić wszystkie węzły w tym samym czasie lub w kilku etapach. Po ponownym
4120 uruchomieniu każdy węzeł serwisowy działa z nowym oprogramowaniem przez okres czasu określony przez
4121 mechanizm aktualizacji oprogramowania. Jeśli ten okres upływa bez odbierania jakichkolwiek potwierdzeń
4122 z węzła podstawowego lub węzeł podstawowy zdecyduje na anulowanie procesu aktualizacji, węzły
4123 serwisowe odrzucą nowe oprogramowanie i przełączą się na nową wersję. W każdym innym przypadku
4124 (odbierany jest komunikat potwierdzenia), węzeł serwisowy uzna nowe oprogramowanie sprzętowe jako
4125 jedyną obowiązującą wersję i usunie stare oprogramowanie.

4126 Odbywa się to w celu pozostawienia „otwartych tylnych drzwi” w razie, gdy nowe oprogramowanie
4127 sprzętowe jest uszkodzone. Należy pamiętać, że węzły serwisowe nie mogą odrzucać żadnej z zapisanych
4128 wersji oprogramowania sprzętowego, aż do ostatecznego potwierdzenia od węzła podstawowego lub do
4129 czasu upływu bezpiecznego okresu. Dwa ostatnie kroki aktualizacji oprogramowania sprzętowego
4130 wyjaśnione powyżej pokazano w punkcie 6.3.5. Patrz punkt 6.3.5.3, aby uzyskać szczegółowy opis
4131 komunikatów kontrolnych.



Rys. 101 - Ponowne uruchamianie węzłów z nowym oprogramowaniem sprzętowym

6.3.3.2 Podział

Obraz oprogramowania sprzętowego zawiera informacje do przesłania w celu przetworzenia aktualizacji oprogramowania. Wielkość obrazu oprogramowania sprzętowego nazwana będzie „*ImageSize*” i jest mierzona w bajtach. Ten obraz jest podzielony na mniejsze elementy, nazywane stronami, które są łatwiejsze do przeniesienia w pakietach. Rozmiar strony „*PageSize*” może wynosić: 32 bajty, 64 bajty, 128 bajtów lub 192 bajtów. Oznacza to, że liczba stron w obrazie oprogramowania sprzętowego jest obliczana według następującego wzoru:

$$PageSize = \left\lceil \frac{ImageSize}{PageSize} \right\rceil + 1$$

Każda strona będzie miała rozmiar określony przez pole *PageSize* poza ostatnią, która będzie zawierać pozostałe bajty do rozmiaru obrazu *ImageSize*.

PageSize jest konfigurowany przez węzeł podstawowy i powiadamiany w czasie inicjalizacji procesu aktualizacji oprogramowania sprzętowego i nakłada warunek w rozmiarze pakietów przenoszonych przez protokół.

6.3.4 Atrybuty PIB oprogramowania sprzętowego

Poniższe atrybuty PIB powinny być obsługiwane przez węzły serwisowe, aby obsłużyć aplikację do pobierania oprogramowania sprzętowego.

Tabela 99 - Atrybuty PIB oprogramowania sprzętowego

Nazwa atrybutu	Rozmiar (w bitach)	ID	Opis
AppFwdlRunning	16	0x0070	Wskazuje czy pobieranie oprogramowania sprzętowego trwa, czy nie. 0 = Brak oprogramowania sprzętowego do pobrania; 1 = Pobieranie oprogramowania sprzętowego w toku.
AppFwdlRxPktCount	16	0x0071	Liczba pakietów pobierania oprogramowania sprzętowego, które zostały odebrane do czasu zapytania.

6.3.5 Mechanizm stanu

6.3.5.1 Ogólne

Węzeł serwisowy korzystający z usługi aktualizacji oprogramowania sprzętowego będzie w jednym z pięciu możliwych stanów: *Brak obciążenia*, *Odbieranie*, *Zakończenie*, *Odliczanie* oraz *Aktualizacja*. Te stany, zdarzenia uruchamiające je i wyniki z nich działania/komunikaty wychodzące zostały opisane poniżej.

Tabela 100 - Mechanizm stanu oprogramowania sprzętowego

Stan aktualizacji	Opis	Zdarzenie	Wartość wyjściowa (lub działanie do wykonania)	Kolejny stan
Brak obciążenia	Aplikacja oprogramowania sprzętowego jest bezczynna.	Odbieranie FU_INFO_REQ	FU_INFO_RSP.	<i>Brak obciążenia</i>
		Odbieranie FU_STATE_REQ	FU_STATE_RSP (.State = 0).	<i>Brak obciążenia</i>
		Odbieranie FU_MISS_REQ	FU_STATE_RSP (.State = 0).	<i>Brak obciążenia</i>
		Odbieranie FU_CRC_REQ	FU_STATE_RSP (.State = 0).	<i>Brak obciążenia</i>
		Odbieranie FU_INIT_REQ	FU_STATE_RSP (.State = 1).	<i>Odbieranie</i>
		Odbieranie FU_DATA	(zignorować).	<i>Brak obciążenia</i>
		Odbieranie FU_EXEC_REQ	FU_STATE_RSP (.State = 0).	<i>Brak obciążenia</i>

Stan aktualizacji	Opis	Zdarzenie	Wartość wyjściowa (lub działanie do wykonania)	Kolejny stan
		Odbieranie FU_CONFIRM_REQ	FU_STATE_RSP (.State = 0).	<i>Brak obciążenia</i>
		Odbieranie FU_KILL_REQ	FU_STATE_RSP (.State = 0).	<i>Brak obciążenia</i>
Odbieranie	Aplikacja oprogramowania sprzętowego odbiera obraz oprogramowania sprzętowego.	Otrzymano pełne oprogramowanie sprzętowe, a kontrola CRC powiodła się.	(Jeśli kontrola CRC pełnego obrazu jest prawidłowa, przełączyć na <i>Zakończenie</i> bez wysyłania dodatkowych komunikatów)	<i>Zakończenie</i>
		Odbieranie FU_INFO_REQ	FU_INFO_RSP.	<i>Odbieranie</i>
		Odbieranie FU_STATE_REQ	FU_STATE_RSP (.State = 1).	<i>Odbieranie</i>
		Odbieranie FU_MISS_REQ	FU_MISS_LIST lub FU_MISS_BITMAP.	<i>Odbieranie</i>
		Odbieranie FU_CRC_REQ	FU_CRC_RSP (FU_STATE_RSP jeśli mapa bitowa nie jest ukończona)	<i>Odbieranie</i>
		Odbieranie FU_INIT_REQ	FU_STATE_RSP (.State = 1)	<i>Odbieranie</i>
		Odbieranie FU_DATA	(odbieranie danych, normalne zachowanie).	<i>Odbieranie</i>
		Odbieranie FU_EXEC_REQ	FU_STATE_RSP (.State = 1).	<i>Odbieranie</i>
		Odbieranie FU_CONFIRM_REQ	FU_STATE_RSP (.State = 1).	<i>Odbieranie</i>
		Odbieranie FU_KILL_REQ	FU_STATE_RSP (.State = 0); (przełączenie na <i>Brak obciążenia</i>).	<i>Brak obciążenia</i>
Zakończenie	Aktualizacja ukończona, integralność obrazu prawidłowa, węzeł serwisowy oczekuje na ponowne uruchomienie z nową wersją oprogramowania.	Odbieranie FU_INFO_REQ	FU_INFO_RSP.	<i>Zakończenie</i>
		Odbieranie FU_STATE_REQ	FU_STATE_RSP (.State = 2).	<i>Zakończenie</i>
		Odbieranie FU_MISS_REQ	FU_STATE_RSP (.State = 2).	<i>Zakończenie</i>
		Odbieranie FU_CRC_REQ	FU_STATE_RSP (.State = 2).	<i>Zakończenie</i>
		Odbieranie FU_INIT_REQ	FU_STATE_RSP (.State = 2).	<i>Zakończenie</i>

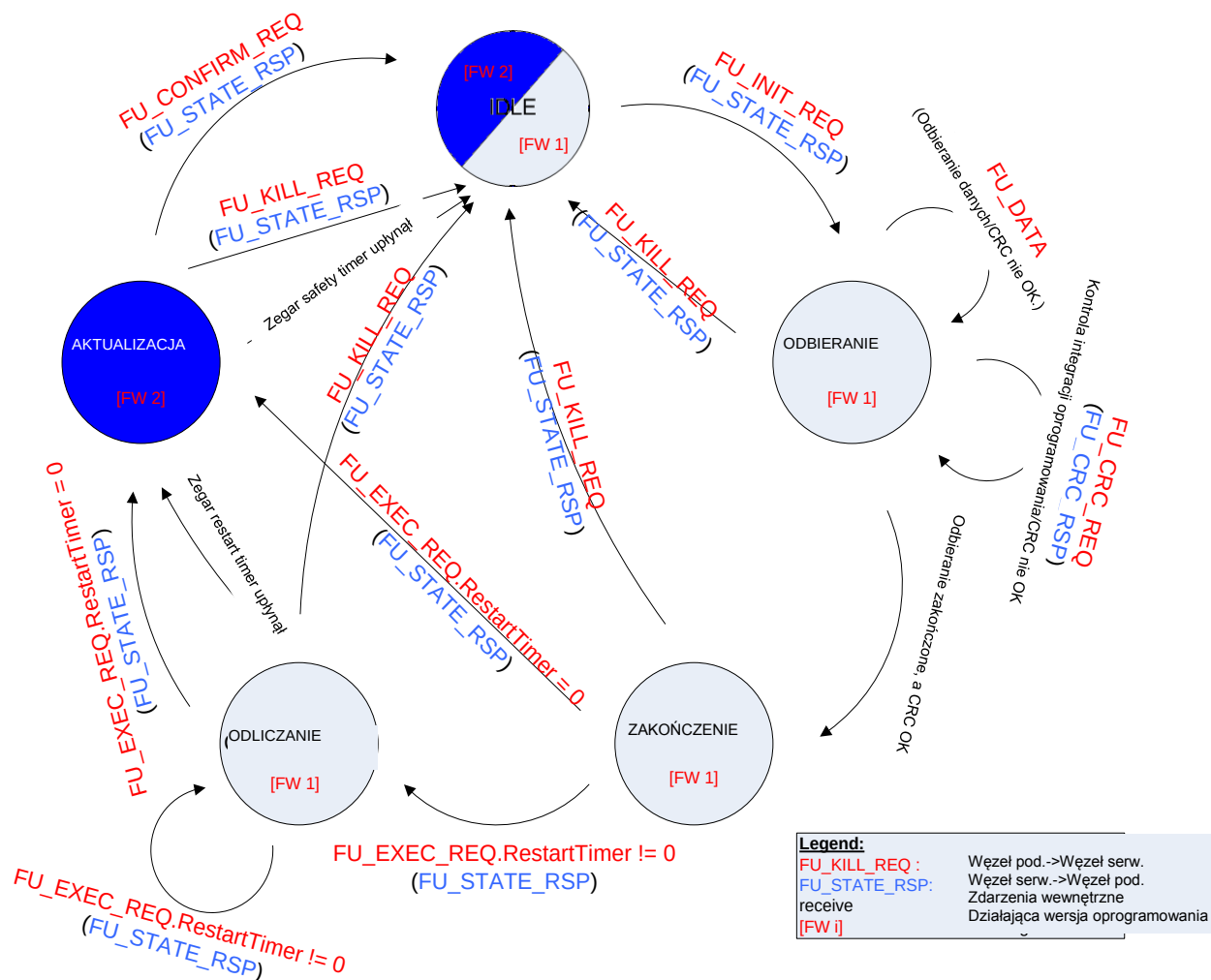
Stan aktualizacji	Opis	Zdarzenie	Wartość wyjściowa (lub działanie do wykonania)	Kolejny stan
		Odbieranie FU_DATA	(zignorować).	Zakończenie
		Odbieranie FU_EXEC_REQ z <i>RestartTimer</i> != 0	FU_STATE_RSP (.State = 3).	Odliczanie
		Odbieranie FU_EXEC_REQ z zegarem <i>RestartTimer</i> = 0	FU_STATE_RSP (.State = 4).	Aktualizacja
		Odbieranie FU_CONFIRM_REQ	FU_STATE_RSP (.State = 2).	Zakończenie
		Odbieranie FU_KILL_REQ	FU_STATE_RSP (.State = 0); (przełączenie na <i>Brak obciążenia</i>).	<i>Brak obciążenia</i>
Odliczanie	Czas do <i>RestartTimer</i> upłynął.	Czas <i>RestartTimer</i> upłynął	(przełączenie na <i>Aktualizacja</i>).	Aktualizacja
		Odbieranie FU_INFO_REQ	FU_INFO_RSP.	Odliczanie
		Odbieranie FU_STATE_REQ	FU_STATE_RSP (.State = 3).	Odliczanie
		Odbieranie FU_MISS_REQ	FU_STATE_RSP (.State = 3).	Odliczanie
		Odbieranie FU_CRC_REQ	FU_STATE_RSP (.State = 3).	Odliczanie
		Odbieranie FU_INIT_REQ	FU_STATE_RSP (.State = 3).	Odliczanie
		Odbieranie FU_DATA	(zignorować).	Odliczanie
		Odbieranie FU_EXEC_REQ z <i>RestartTimer</i> != 0	FU_STATE_RSP (.State = 3); (aktualizacja <i>RestartTimer</i> i <i>SafetyTimer</i>).	Odliczanie
		Odbieranie FU_EXEC_REQ przy zegarze <i>RestartTimer</i> = 0	FU_STATE_RSP (.State = 4); (aktualizacja <i>RestartTimer</i> i <i>SafetyTimer</i>).	Aktualizacja
		Odbieranie FU_CONFIRM_REQ	FU_STATE_RSP (.State = 3).	Odliczanie
		Odbieranie FU_KILL_REQ	FU_STATE_RSP (.State = 0); (przełączenie na <i>Brak obciążenia</i>).	<i>Brak obciążenia</i>
Aktualizacja	Mechanizm aktualizacji oprogramowania	Czas <i>SafetyTimer</i> upłynął	FU_STATE_RSP (.State = 0); (przełączanie na <i>Brak obciążenia</i>).	<i>Brak obciążenia</i>

Stan aktualizacji	Opis	Zdarzenie	Wartość wyjściowa (lub działanie do wykonania)	Kolejny stan
	sprzętowego uruchamia się ponownie za pomocą obrazu oprogramowania firmowego i sprawdza je przez <i>SafetyTimer</i> sekund.	Odbieranie FU_INFO_REQ	FU_INFO_RSP.	<i>Aktualizacja</i>
		Odbieranie FU_STATE_REQ	FU_STATE_RSP (.State = 4).	<i>Aktualizacja</i>
		Odbieranie FU_MISS_REQ	FU_STATE_RSP (.State = 4).	<i>Aktualizacja</i>
		Odbieranie FU_CRC_REQ	FU_STATE_RSP (.State = 4).	<i>Aktualizacja</i>
		Odbieranie FU_INIT_REQ	FU_STATE_RSP (.State = 4).	<i>Aktualizacja</i>
		Odbieranie FU_DATA	(zignorować).	<i>Aktualizacja</i>
		Odbieranie FU_EXEC_REQ	FU_STATE_RSP (.State = 0).	<i>Aktualizacja</i>
		Odbieranie FU_CONFIRM_REQ	FU_STATE_RSP (.State = 0); (przełączanie na <i>Brak obciążenia</i> , oprogramowanie zatwierdzone).	<i>Brak obciążenia</i>
		Odbieranie FU_KILL_REQ	FU_STATE_RSP (.State = 0); (przełączanie na <i>Brak obciążenia</i>).	<i>Brak obciążenia</i>

4161

4162

4163 Diagram stanów przedstawiono poniżej. Należy zauważyć, że diagram pokazuje tylko najważniejsze
 4164 zdarzenia. Szczegółowy opis zachowania każdego stanu i zdarzeń oraz związanych z nimi działań znajduje
 4165 się w punkcie 6.3.5.3. Krótki opis każdego stanu przedstawiono w punkcie 6.3.5.2.



Rys. 102 - Mechanizm aktualizacji oprogramowania sprzętowego, diagram stanu

6.3.5.2 Opis stanu

6.3.5.2.1 Brak obciążenia

Podczas przeprowadzania aktualizacji oprogramowania sprzętowego, węzły serwisowe są w stanie *Braku obciążenia*. Odbiór komunikatu **FU_INIT_REQ** to jedyne zdarzenie wymuszające przełączenie węzła serwisowego w kolejny stan (*Odbieranie*). **FU_KILL_REQ** anuluje proces aktualizacji i wymusza od węzła serwisowego przełączenie z dowolnego stanu na „Brak obciążenia”.

6.3.5.2.2 Odbieranie

Węzeł serwisowy odbiera obraz oprogramowania sprzętowego za pośrednictwem komunikatów **FU_DATA**. Po zakończeniu pobierania integralność obrazu sprawdzana jest przez węzeł podstawowy za pomocą **FU_CRC_REQ**, a węzeł serwisowy odpowie za pomocą **FU_CRC_RSP**. Ostateczna kontrola CRC pełnego

4179 obrazu oprogramowania sprzętowego jest obowiązkowa. Jeśli kontrola CRC będzie pomyślna, węzeł
4180 serwisowy odpowie za pomocą FU_CRC_RSP, a następnie przełączy się w stan *Zakończenie*. Jeśli kontrola
4181 CRC nie powiedzie się, węzeł serwisowy odpowie węzłowi podstawowemu za pośrednictwem FU_CRC_RSP,
4182 rzuci pełny obraz oprogramowania sprzętowego, zaktualizuje mapę bitową i będzie oczekiwać na
4183 retransmisję pakietu.

4184 Proszę pamiętać, że węzeł serwisowy zmieni się ze stanu *Odbieranie* na *Zakończenie* jedynie, jeśli pobrano
4185 pełny obraz oprogramowania sprzętowego, a kontrola CRC powiodła się.

4186 6.3.5.2.3 Zakończenie

4187 Węzeł serwisowy w stanie *Zakończenie* czeka aż do odbioru komunikatu FU_EXEC_REQ. Węzeł serwisowy
4188 może przełączyć się albo w stan *Odliczanie* lub *Aktualizacja*, w zależności od pola *RestartTimer*, które
4189 określa, które wystąpienie węzła serwisowego musi się ponownie uruchomić za pomocą nowego
4190 oprogramowania. Jeśli czas zegara *RestartTimer* = 0, węzeł serwisowy natychmiast przełącza się w stan
4191 *Aktualizacja*; w przeciwnym razie przełącza się w stan *Odliczanie*.

4192 6.3.5.2.4 Odliczanie

4193 Węzeł serwisowy w stanie *Odliczanie* odczekuje czas określony w polu zegara *RestartTimer* poprzedniego
4194 komunikatu FU_EXEC_REQ. Po upływie tego czasu status automatycznie zmienia się na „*Aktualizacja*”.

4195 FU_EXEC_REQ można zastosować w stanie „*Odliczanie*” do zresetowania *RestartTimer* i *SafetyTimer*. W tym
4196 przypadku oba zegary należy określić w FU_EXEC_REQ, ponieważ oba zostaną nadpisane. Należy zauważyć,
4197 że możliwe jest wymuszenie od węzła natychmiastowego przełączenia się ze stanu *Odliczanie* do stanu
4198 *Aktualizacja* poprzez ustawienie wartości *RestartTimer* na zero.

4199 6.3.5.2.5 Aktualizacja

4200 Węzeł serwisowy w stanie *Aktualizacja* powinien uruchomić nowe oprogramowanie sprzętowe w czasie
4201 określonym przez zegar FU_EXEC_REQ.SafetyTimer. Jeśli nie odbiera on żadnych potwierdzeń przed
4202 upływem tego czasu (lub jeśli odbiera on komunikat FU_KILL_REQ), węzeł serwisowy odrzuca nowe
4203 oprogramowanie sprzętowe, uruchamia się ponownie ze starą wersją i przełącza na stan „*Braku*
4204 *obciążenia*”. W każdym innym wypadku odrzuca on starą wersję oprogramowania i przełącza się w stan
4205 „*Brak obciążenia*”.

4206 6.3.5.3 Pakiety kontrolne

4207 6.3.5.3.1 FU_INIT_REQ

4208 Węzeł podstawowy wysyła ten pakiet, aby skonfigurować węzeł serwisowy dla aktualizacji oprogramowania
4209 sprzętowego. Jeśli węzeł serwisowy jest w stanie *Braku obciążenia*, zmieni się on z tego stanu na *Odbieranie*
4210 i odpowie za pomocą FU_STATE_RSP. W każdym przypadku odpowiedź nastąpi za pomocą FU_STATE_RSP.

4211 Treść FU_INIT_REQ pokazano poniżej.

4212

4213 Tabela 101 - Pola FU_INIT_REQ

Pole	Długość	Opis
Type	4 bity	0 = FU_INIT_REQ.
Version	2 bity	0 dla tej wersji protokołu.
PageSize	2 bity	0 dla rozmiaru strony PageSize=32; 1 dla rozmiaru strony PageSize=64; 2 dla rozmiaru strony PageSize=128; 3 dla rozmiaru strony PageSize=192;
ImageSize	32 bity	Rozmiar obrazu Aktualizacji Oprogramowania sprzętowego w bajtach.
CRC	32 bity	Kod CRC obrazu aktualizacji oprogramowania sprzętowego. Wielomian wejściowy $M(x)$ ma postać wielomianu którego współczynniki są sprawdzanymi bitami danych (pierwszy bit do sprawdzenia jest najwyższym współczynnikiem korelacji, a ostatni bit do sprawdzenia jest współczynnikiem korelacji zerowej. Wielomian generujący dla CRC wynosi $G(x)=x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^5+x^4+x^2+x+1$. Reszta $R(x)$ jest obliczona jako reszta z dzielenia $M(x) \cdot x^{32}$ przez $G(x)$. Współczynniki reszty będą następnie wynikową kontrolą CRC.

4214 6.3.5.3.2 FU_EXEC_REQ

4215 Ten pakiet jest używany przez węzeł podstawowy, aby nakazać węzłowi serwisowemu w stanie *Zakończenie*
 4216 ponowne uruchomienie za pomocą nowego oprogramowania sprzętowego, gdy węzeł serwisowy odebrał
 4217 ukończony obraz. FU_EXEC_REQ określa, kiedy węzeł serwisowy musi ponownie się uruchomić i jak długo
 4218 powinien trwać „bezpieczny” okres, jak wyjaśniono w punkcie 6.3.5.2.5. Dodatkowo FU_EXEC_REQ można
 4219 zastosować w stanie „Odliczanie” do zresetowania zegarów *RestartTimer* i *SafetyTimer*.

4220 W zależności od wartości zegara *RestartTimer* węzeł serwisowy w stanie *Zakończenie* może zmienić się na
 4221 *Odliczanie* lub *Aktualizacja*. W każdym przypadku węzeł serwisowy odpowiada za pomocą FU_STATE_RSP.

4222 W stanie „Odliczanie” węzeł podstawowy może wyzerować zegar *RestartTimer* i *SafetyTimer* za pomocą
 4223 komunikatu FU_EXEC_REQ (oba zegary muszą być określone w komunikacie, ponieważ oba zostaną
 4224 nadpisane).

4225 Zawartość tego pakietu opisano poniżej.

4226 Tabela 102 - Pola FU_EXEC_REQ

Pole	Długość	Opis
Type	4 bity	1 = FU_EXEC_REQ.

Pole	Długość	Opis
Version	2 bity	0 dla tej wersji protokołu.
Reserved	2 bity	0 .
RestartTimer	16 bitów	0..65536 sekund; czas przed restartem z nowym oprogramowaniem sprzętowym.
SafetyTimer	16 bitów	0..65536 sekund; czas do testu z nowym oprogramowaniem sprzętowym. Czas rozpoczyna się wraz z wprowadzeniem stanu „Aktualizacja”.

4227

4228 **6.3.5.3.3 FU_CONFIRM_REQ**

4229 Pakiet ten wysyłany jest przez Węzeł podstawowy do Węzła serwisowego w stanie „Aktualizacja”, aby
 4230 zatwierdzić bieżące oprogramowanie sprzętowe. Jeśli węzeł serwisowy odbierze ten komunikat, odrzuca on
 4231 starą wersję oprogramowania i przełącza się w stan „Brak obciążenia”. Podczas odbierania tego komunikatu
 4232 węzeł serwisowy odpowiada za pomocą FU_STATE_RSP.

4233 W każdym innym stanie węzeł serwisowy odpowiada za pomocą FU_STATE_RSP bez wykonywania innych
 4234 dodatkowych działań.

4235 Pakiet ten zawiera pola opisane poniżej.

4236 **Tabela 103 - Pola FU_CONFIRM_REQ**

Pole	Długość	Opis
Type	4 bity	2 = FU_CONFIRM_REQ.
Version	2 bity	0 dla tej wersji protokołu.
Reserved	2 bity	0 .

4237 **6.3.5.3.4 FU_STATE_REQ**

4238 Pakiet ten wysyłany jest przez Węzeł podstawowy, aby uzyskać stan Aktualizacji oprogramowania
 4239 sprzętowego Węzła serwisowego. Węzeł serwisowy odpowie za pomocą FU_STATE_RSP.

4240 Pakiet ten zawiera pola opisane poniżej.

4241 **Tabela 104 - Pola FU_STATE_REQ**

Pole	Długość	Opis
Type	4 bity	3 = FU_STATE_REQ.
Version	2 bity	0 dla tej wersji protokołu.

Pole	Długość	Opis
<i>Reserved</i>	2 bity	0.

4242

4243 **6.3.5.3.5 FU_KILL_REQ**

4244 Węzeł podstawowy wysyła ten komunikat, aby zakończyć proces aktualizacji oprogramowania
 4245 sprzętowego. Węzeł serwisowy odbierający ten komunikat automatycznie przełączy się w stan „*Brak*
 4246 *obciążenia*” i opcjonalnie usunie pobrane dane. Węzeł serwisowy odpowiada wysyłając FU_STATE_RSP.

4247 Zawartość tego pakietu opisano poniżej.

4248

Tabela 105 - Pola FU_KILL_REQ

Pole	Długość	Opis
Type	4 bity	4 = FU_KILL_REQ.
Version	2 bity	0 dla tej wersji protokołu.
<i>Reserved</i>	2 bity	0.

4249 **6.3.5.3.6 FU_STATE_RSP**

4250 Pakiet ten wysyłany jest przez Węzeł serwisowy jako odpowiedź na komunikaty FU_STATE_REQ,
 4251 FU_KILL_REQ, FU_EXEC_REQ, FU_CONFIRM_REQ lub FU_INIT_REQ odebrane przez połączenie unicast.
 4252 Służy do powiadamiania o stanie aktualizacji oprogramowania w węźle serwisowym.

4253 Dodatkowo FU_STATE_RSP jest stosowany jako domyślna odpowiedź na wszystkie zdarzenia, które
 4254 występują w stanach, gdzie nie są przewidziane (np. FU_EXEC_REQ w stanie *Odbieranie*, FU_INIT_REQ w
 4255 stanie *Aktualizacja*..).

4256 Pakiet ten zawiera pola opisane poniżej.

4257

Tabela 106 - Pola FU_STATE_RSP

Pole	Długość	Opis
Type	4 bity	5 = FU_STATE_RSP.
Version	2 bity	0 dla tej wersji protokołu.
Reserved	2 bity	0.
State	4 bity	0 dla Braku obciążenia; 1 dla Odbierania; 2 dla Kończenia;

Pole	Długość	Opis
		3 dla Odliczania; 4 dla Aktualizacji; 5 do 15 zarezerwowane do użytku w przyszłości.
Reserved	4 bity	0.
CRC	32 bity	CRC jako kontrola otrzymana w polu CRC pakietu FU_INIT_REQ.
Received	32 bity	Liczba odebranych stron (to pole powinno istnieć jedynie jeśli stan ustawiony jest na Odbieranie).

4258 6.3.5.3.7 FU_DATA

4259 Pakiet ten wysyłany jest przez Węzeł podstawowy w celu przeniesienia strony obrazu oprogramowania
4260 sprzętowego do węzła serwisowego. Odpowiedź z węzła podstawowego nie jest oczekiwana.

4261 Pakiet ten zawiera pola opisane poniżej.

4262 Tabela 107 - Pola FU_DATA

Pole	Długość	Opis
Type	4 bity	6 = FU_DATA.
Version	2 bity	0 dla tej wersji protokołu.
Reserved	2 bity	0.
PageIndex	32 bity	Indeks przesyłanej strony.
Reserved	8 bitów	Bajt wypełnienia dla urządzeń 16-bitowych. Domyślnie ustawiony na 0.
Data	Zmienna	Dane strony. Długość tych danych jest równa rozmiarowi PageSize (32, 64, 128 lub 192 bajtów) dla każdej strony, poza ostatnią, która będzie miała rozmiar równy pozostałym bajtom obrazu.

4263 6.3.5.3.8 FU_MISS_REQ

4264 Pakiet ten wysyłany jest przez Węzeł podstawowy w celu zażądania informacji na temat stron, które w
4265 dalszym ciągu mają zostać odebrane.

4266 Jeśli węzeł serwisowy jest w stanie *Odbieranie*, odpowie on za pomocą komunikatu FU_MISS_BITMAP lub
4267 FU_MISS_LIST. Jeśli węzeł serwisowy jest w innym stanie, odpowie on za pomocą FU_STATE_RSP.

4268 Pakiet ten zawiera pola opisane poniżej.

4269

Tabela 108 - Pola FU_MISS_REQ

Pole	Długość	Opis
Type	4 bity	7 = FU_MISS_REQ.
Version	2 bity	0 dla tej wersji protokołu.
Reserved	2 bity	0.
PageIndex	32 bity	Punkt wyjścia do zbierania informacji na temat brakujących stron.

4270 **6.3.5.3.9 FU_MISS_BITMAP**

4271 Pakiet ten wysyłany jest przez Węzeł serwisowy jako odpowiedź na FU_MISS_REQ. Przenosi on informacje
 4272 na temat stron, które w dalszym ciągu muszą być odebrane.

4273 Ten pakiet będzie zawierał pola opisane poniżej.

4274 Tabela 109 - Pola FU_MISS_BITMAP

Pole	Długość	Opis
Type	4 bity	8 = FU_MISS_BITMAP.
Version	2 bity	0 dla tej wersji protokołu.
Reserved	2 bity	0.
PageIndex	32 bity	Indeks strony reprezentowany przez pierwszy bit mapy bitowej. Powinien być taki sam jak pole <i>PageIndex</i> field w komunikatach FU_MISS_REQ lub poprzedni. Jeśli jest późniejszy, oznacza to, że strony pomiędzy nimi są już odebrane. W tym przypadku, jeśli odebrane zostały wszystkie strony po <i>PageIndex</i> określonym w FU_MISS_REQ, węzeł serwisowy powinien rozpocząć wyszukiwanie od początku (<i>PageIndex</i> = 0).
Bitmap	Zmienna	Ta mapa bitowa zawiera informacje na temat statusu każdej strony. Pierwszy bit (najbardziej znaczący bit pierwszego bajta) reprezentuje status strony określonej przez <i>PageIndex</i> . Kolejny bit oznacza status <i>PageIndex+1</i> , itd. „1” oznacza, że brakuje strony, a „0” oznacza, że strona została już odebrana. Po bicie oznaczającym ostatnią stronę obrazu możliwe jest przepełnienie za pomocą bitów, które reprezentują brakujący status strony z indeksem zero. Maksymalna długość tego pola wynosi <i>PageSize</i> .

4275 Od węzła serwisowego zależy podjęcie decyzji o wysłaniu tego typu pakietu lub komunikatu FU_MISS_LIST.
 4276 Zazwyczaj bardziej skuteczne jest przesyłanie tego rodzaju pakietów, gdy liczba brakujących pakietów nie

4277 jest bardzo niska. Ale od wdrożenia zależy wybór pakietu do przestania. Węzeł podstawowy powinien
4278 zrozumieć oba.

4279 6.3.5.3.10 FU_MISS_LIST

4280 Pakiet ten wysyłany jest przez Węzeł serwisowy jako odpowiedź na FU_MISS_REQ. Przenosi on informacje
4281 na temat stron, które w dalszym ciągu muszą być odebrane.

4282 Ten pakiet będzie zawierał pola opisane poniżej.

4283 Tabela 110 - Pola FU_MISS_LIST

Pole	Długość	Opis
Type	4 bity	9 = FU_MISS_LIST.
Version	2 bity	0 dla tej wersji protokołu.
Reserved	2 bity	0.
PageIndexList	Zmienna	Lista stron, które w dalszym ciągu mają zostać odebrane. Każda strona jest reprezentowana przez PageIndex, zaszyfrowany jako 32-bitowa liczba całkowita. Te strony powinny być sortowane w porządku rosnącym (od najniższego do najwyższego), aby możliwe było przepełnienie do PageIndex równe zero i kontynuowanie od początku. Pierwszy indeks strony powinien być taki sam jak pole PageIndex field w komunikatach FU_MISS_REQ lub poprzedni. Jeśli jest późniejszy, oznacza to, że strony pomiędzy nimi są już odebrane (możliwe jest przepełnienie indeksu strony i rozpoczęcie od początku). Maksymalna długość tego pola wynosi PageSize.

4284 Od węzła serwisowego zależy podjęcie decyzji o wysłaniu tego typu pakietu lub komunikatu
4285 FU_MISS_BITMAP. Zazwyczaj bardziej skuteczne jest przysyłanie tego rodzaju pakietów, gdy brakujące
4286 pakiety są bardzo rzadkie, ale to od wdrożenia zależy wybór pakietu do wysłania. Węzeł podstawowy
4287 powinien zrozumieć oba.

4288 6.3.5.3.11 FU_INFO_REQ

4289 Pakiet ten wysyłany jest przez Węzeł podstawowy w celu zażądania informacji od węzła serwisowego,
4290 takich jak nazwa producenta, model urządzenia, wersja oprogramowania i inne parametry określone przez
4291 producenta. Węzeł serwisowy odpowie za pomocą pakietów FU_INFO_RSP.

4292 Pakiet ten zawiera pola opisane poniżej.

4293

4294 Tabela 111 - Pola FU_INFO_REQ

Pole	Długość	Opis
Type	4 bity	10 = FU_INFO_REQ.
Version	2 bity	0 dla tej wersji protokołu.
Reserved	2 bity	0.
InfoldList	Zmienna	Lista identyfikatorów zawierających informacje do odzyskania. Długość każdego identyfikatora wynosi 1 bajt. Maksymalna długość tego pola to 32 bajty.

4295 Definiuje się następujące identyfikatory:

4296 **Tabela 112 - Wartości dodatnie Infold**

Infold	Nazwa	Opis
0	Manufacturer	Uniwersalny identyfikator Producenta.
1	Model	Model produktu działającego jako Węzeł serwisowy.
2	Firmware	Aktualnie wykonywana wersja oprogramowania sprzętowego.
128-255	<i>Manufacturer specific</i>	Zakres wartości, które są właściwe dla danego producenta.

4297

4298 **6.3.5.3.12 FU_INFO_RSP**

4299 Pakiet ten wysyłany jest przez węzeł serwisowy jako odpowiedź na komunikat węzła podstawowego
 4300 FU_INFO_REQ. Węzeł serwisowy może musieć wysłać więcej niż jedną odpowiedź FU_INFO_RSP podczas
 4301 odpowiadania na żądanie wysłane przez węzeł podstawowy.

4302 Pakiet ten zawiera pola opisane poniżej.

4303 **Tabela 113 - Pola FU_INFO_RSP**

Pole	Długość	Opis
Type	4 bity	11 = FU_INFO_RSP.
Version	2 bity	0 dla tej wersji protokołu.
Reserved	2 bity	0.
InfoData	0 – 192 bajtów	Dane z informacjami wymaganymi przez węzeł podstawowy. Mogą one zawierać kilka pozycji (jedną dla każdego wymaganego identyfikatora). Każda pozycja ma maksymalny rozmiar 32 bajtów. Maksymalna długość tego pola to 192 bajty (6 pozycji).

4304 Pole InfoData może zawierać kilka pozycji. Format każdej pozycji określono poniżej.

4305 **Tabela 114 - Pola każdej pozycji InfoData w FU_INFO_RSP**

Pole	Długość	Opis
Infold	8 bitów	Identyfikator informacji określonych w punkcie 6.3.5.3.11.
<i>Reserved</i>	3 bity	0.
Length	5 bitów	Długość pola danych <i>Data</i> (jeśli długość wynosi 0, oznacza to, że określone pole Infold nie jest obsługiwane przez dane urządzenie).
Data	0 – 30 bajtów	Dane z informacjami dostarczonymi przez węzeł serwisowy. Ich zawartość może zależeć od znaczenia pola Infold. Żadna wartość nie może być dłuższa niż 30 bajtów.

4306 **6.3.5.3.13 FU_CRC_REQ**

4307 FU_CRC_REQ jest wysyłany przez węzeł podstawowy do nakazania węzłowi serwisowemu wykonania
 4308 kontroli CRC na pełnym obrazie oprogramowania sprzętowego. Kontrola CRC pełnego obrazu
 4309 oprogramowania sprzętowego jest obowiązkowa. Kontrola CRC określona w FU_CRC_REQ.CRC jest taka
 4310 sama, jak w FU_INIT_REQ.

4311 Węzeł serwisowy odpowiada za pomocą FU_CRC_RSP jeśli znajduje się w stanie *Odbieranie*; w innym
 4312 przypadku odpowiada za pomocą FU_STATE_RSP. Węzeł podstawowy nie powinien wysłać FU_CRC_REQ
 4313 jeśli pobieranie obrazu nie zostało zakończone (to jest mapa bitowa nie jest ukończona). W razie, gdy węzeł
 4314 podstawowy zachowuje się nieprawidłowo i wysyła FU_CRC_REQ przed ukończeniem pobierania
 4315 oprogramowania sprzętowego, węzeł serwisowy powinien odpowiedzieć za pomocą FU_STATE_RSP.

4316 Należy zauważyć, że w stanie *Braku obciążenia* pole kontroli CRC z FU_STATE_RSP będzie elementem
 4317 fikcyjnym (ponieważ nie odebrano jeszcze żadnego prymitywu FU_INIT_REQ). Węzeł podstawowy zignoruje
 4318 to pole, jeśli węzeł serwisowy znajduje się w stanie „Braku obciążenia”.

4319 Pakiet ten zawiera pola opisane poniżej.

4320 **Tabela 115 - Pola FU_CRC_REQ**

Pole	Długość	Opis
Type	4 bity	12 = FU_CRC_REQ.
Version	2 bity	0 dla tej wersji protokołu.
<i>Reserved</i>	2 bity	0.
SectionSize	32 bity	Rozmiar obrazu Aktualizacji Oprogramowania sprzętowego w bajtach.

Pole	Długość	Opis
CRC	32 bity	Kod CRC obrazu aktualizacji oprogramowania sprzętowego. Wielomian wejściowy $M(x)$ ma postać wielomianu którego współczynniki są sprawdzanymi bitami danych (pierwszy bit do sprawdzenia jest najwyższym współczynnikiem korelacji, a ostatni bit do sprawdzenia jest współczynnikiem korelacji zerowej. Wielomian generujący dla CRC wynosi $G(x)=x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^5+x^4+x^2+x+1$. Reszta $R(x)$ jest obliczona jako reszta z dzielenia $M(x) \cdot x^{32}$ przez $G(x)$. Współczynniki reszty będą następnie wynikową kontrolą CRC.

4321 6.3.5.3.14 FU_CRC_RSP

4322 Pakiet ten wysyłany jest przez węzeł serwisowy jako odpowiedź na komunikat węzła podstawowego
 4323 FU_CRC_REQ.

4324 Pakiet ten zawiera pola opisane poniżej.

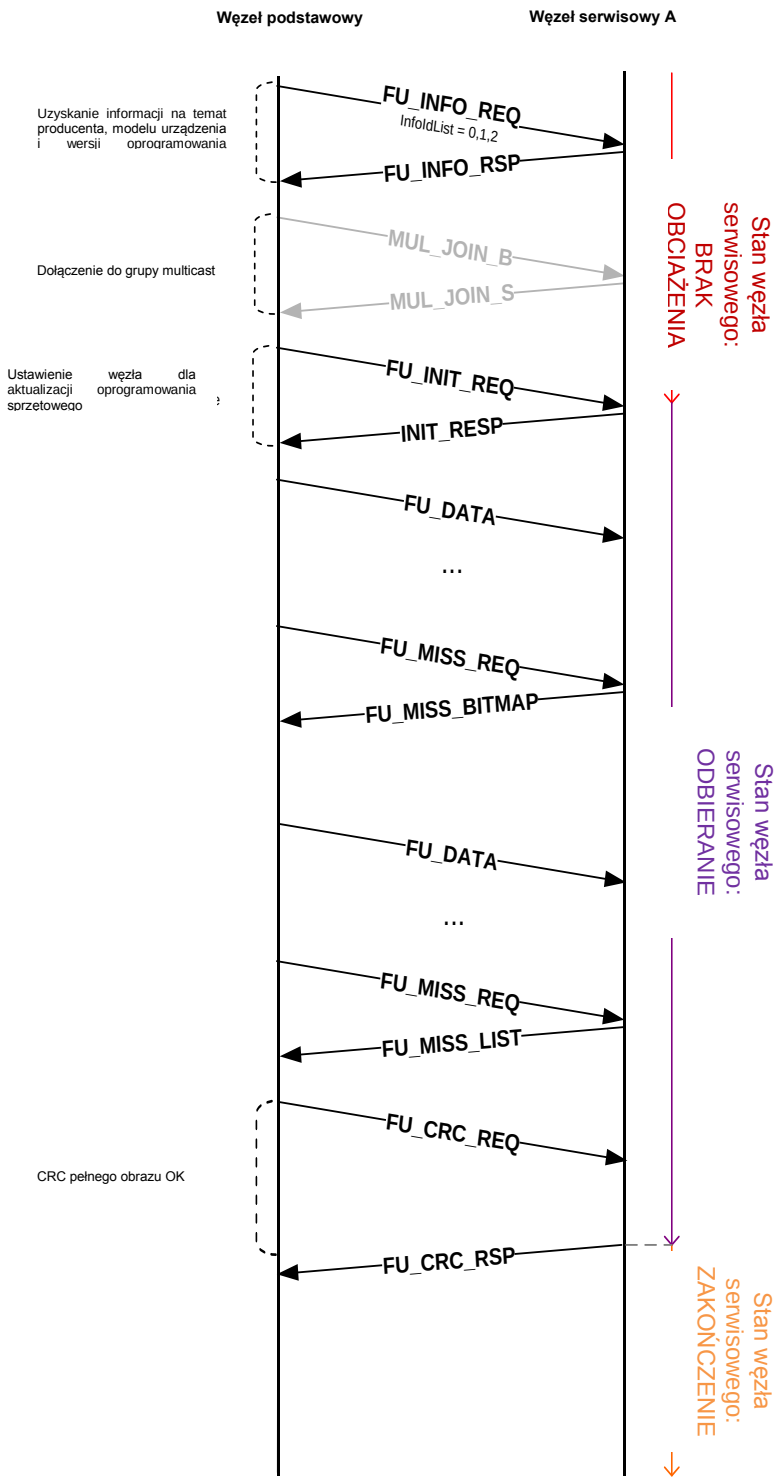
4325 Tabela 116 - Pola FU_CRC_RSP

Pole	Długość	Opis
Type	4 bity	13 = FU_CRC_RSP.
Version	2 bity	0 dla tej wersji protokołu.
CRC_Result	1 bit	Wynik kontroli CRC: „0” - niepowodzenie kontroli; „1” - powodzenie kontroli.
Reserved	1 bit	0.

4326

6.3.6 Przykłady

Poniższe rysunki stanowią przykład ruchu wygenerowanego pomiędzy węzłem podstawowym a węzłem serwisowym w trakcie procesu aktualizacji oprogramowania.

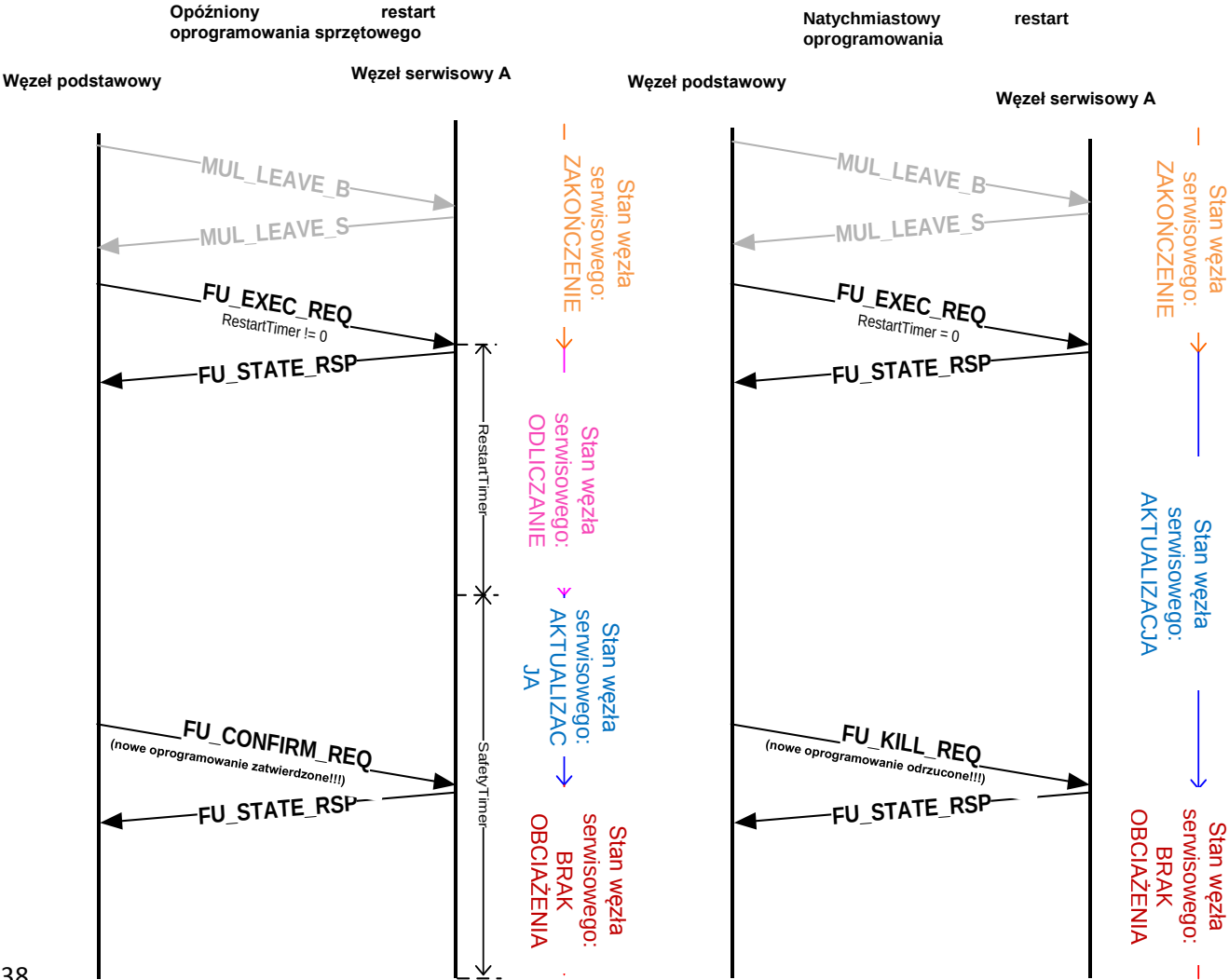


Rys. 103 - Inicjalizacja Węzła serwisowego i pełny obraz oprogramowania sprzętowego

Powyższy rysunek pokazuje inicjalizację procesu, pobieranie oprogramowania sprzętowego i kontrolę integralności obrazu. W powyższym przykładzie pobrany obraz oprogramowania powinien zostać

4334 ukończony przed wystaniem ostatniego żądania FU_MISS_REQ. Węzeł podstawowy wysyła go celem
4335 weryfikacji jego mapy bitowej. W tym przykładzie FU_MISS_LIST ma puste pole *PageIndexList* field, co
4336 oznacza, że obraz oprogramowania sprzętowego jest pełny.

4337



4338

4339 **Rys. 104 - Przeprowadzanie aktualizacji i zatwierdzenie/odrzućenie nowej wersji oprogramowania**

4340 Powyżej pokazano jak postępować po zakończeniu pobierania oprogramowania sprzętowego. Węzeł
4341 podstawowy nakazuje węzłowi serwisowemu ponowne uruchomienie albo natychmiast („Natychmiastowe
4342 uruchomienie oprogramowania sprzętowego”, *RestartTimer* = 0) lub po określonym czasie („Opóźnione
4343 uruchomienie oprogramowania sprzętowego”, *RestartTimer* != 0). Po ponownym uruchomieniu węzeł
4344 podstawowy może albo potwierdzić niedawno pobrany komunikat wysyłając **FU_CONFIRM_REQ** lub
4345 odrzucić go (wysyłając **FU_KILL_REQ** lub pozwalając na upływanie bezpiecznego okresu i nie robiąc nic).

4346

6.4 Opis interfejsu zarządzania

6.4.1 Ogólne

Funkcje zarządzania określone w poprzednich rozdziałach są dostępne w abstrakcyjnym interfejsie zarządzania opisanym w niniejszym punkcie. Interfejs może być dostępny przez różne media. Każdy nośnik fizyczny powinien określić swój profil komunikacji płaszczyzny zarządzania, przez który wymieniane będą informacje zarządzania. Jest on obowiązkowy dla implementacji w celu obsługi profilu komunikacji płaszczyzny zarządzania PRIME. Wszystkie pozostałe „profile komunikacji płaszczyzny zarządzania” są opcjonalne i mogą być nakazane do zastosowania w określonych przypadkach przez określone „profile aplikacji”.

Aktualna wersja specyfikacji opisuje dwa profile komunikacji: komunikację przez zerową podwarstwę SSCS oraz komunikację przez łącze szeregowo.

Dzięki tym dwóm profilom komunikacji powinno być możliwe postępowanie z następującymi przypadkami:

1. Dostęp zdalny interfejsu zarządzania przez zerową warstwę SSCS. Powinno to umożliwić użycie węzła podstawowego jako bramy nadzorującej wszystkie urządzenia w podsieci.
2. Lokalny dostęp do interfejsu zarządzania (przez urządzenia peryferyjne, takie jak RS232, USB-port szeregowy, itd.) w węźle serwisowym. Lokalny dostęp powinien być możliwy w przypadkach, gdy koprocessor służy do kontroli nadzorczej procesora lub gdy dla celów konserwacji wymagany jest ręczny dostęp do lokalnego interfejsu fizycznego.

Dane zarządzania składają się z 2-bajtowego nagłówka, po którym następują informacje o treści odpowiadające typowi informacji przenoszonych w komunikacie. Nagłówek składa się z pola o długości 10 bitów i pola identyfikatora komunikatu o długości 6 bitów.

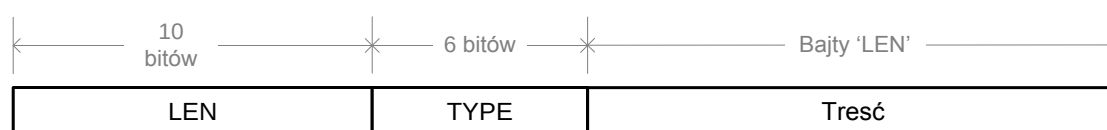


Tabela 117 - Zarządzanie danymi z pól

Nazwa	Długość	Opis
MGMT.LEN	10 bitów	Długość danych treści po 2-bajtowym nagłówku. LEN=0 oznacza, że za tym nagłówkiem nie ma już żadnych danych treści oraz że pole TYPE zawiera wszystkie informacje wymagane do podjęcia odpowiednich działań. UWAGA: Pole długości może zbędne w przypadku niektórych profili komunikacji (np. podczas przesyłania w OFDM PRIME), ale jest wymagane w przypadku innych profili. Dlatego dla zachowania jednolitości, jest ona zawsze wliczana w zarządzaniu danymi.

Nazwa	Długość	Opis
MGMT.TYPE	6 bitów	Typ informacji zarządzania przesyłanych w odpowiednich danych. Część identyfikatorów komunikatów ma standardową semantykę, która powinna być respektowana przez wszystkie urządzenia zgodne z OFMD PRIME, podczas gdy inne zarezerwowane są dla lokalnego wykorzystania przez dostawców. 0x00 – Uzyskiwanie zapytania atrybutu PIB; 0x01 – Uzyskiwanie odpowiedzi atrybutu PIB; 0x02 – Ustawianie żądania atrybutu PIB; 0x03 – Resetowanie wszystkich atrybutów statystyk PIB; 0x04 – Restartowanie urządzenia docelowego; 0x05 – Komunikat protokołu aktualizacji oprogramowania sprzętowego; 0x06 – 0x0F: Zarezerwowany do użytku w przyszłości. Dostawcy nie powinni stosować tych wartości dla celów lokalnych; 0x10 – 0x3F : Zarezerwowany dla użytku właściwego dla dostawców.

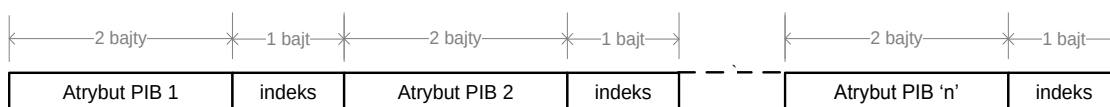
4371 6.4.2 Format treści informacji zarządzania

4372 6.4.2.1 Uzyskiwanie (GET) zapytania atrybutu PIB

4373 Zapytanie to jest wysyłane przez jednostkę zdalnego zarządzania, która chce znać wartości atrybutów PIB
 4374 utrzymywane na zgodnym urządzeniu stosującym niniejszą specyfikację.

4375 Treść może składać się z zapytania dotyczącego albo pojedynczego atrybutu PIB lub wielu atrybutów. Ze
 4376 względu na wydajność, zapytania na wielu atrybutach PIB mogą być łączone w pojedyncze polecenie. Biorąc
 4377 pod uwagę, że identyfikator atrybutu PIB jest stały, liczba atrybutów wnioskowanych w pojedynczym
 4378 poleceniu wyprowadzana jest z ogólnego pola MGMT.LEN w nagłówku.

4379 Format informacji o treści pokazano na kolejnym rysunku.



4380

4381 Pola żądania GET streszczone zostały w tabeli poniżej:

4382 **Tabela 118 - Pola żądania atrybutu PIB GET**

Nazwa	Długość	Opis
PIB Attribute id	2 bajty	16-bitowy identyfikator atrybutu PIB

Nazwa	Długość	Opis
Index	1 bajt	Indeks pozycji zwracanych dla odpowiedniego identyfikatora Atrybutu PIB. To pole jest prawidłowe jedynie podczas zwracania atrybutów listy bazy informacji PLC. Index = 0; jeśli atrybut PIB nie jest listą; Index = 1 do 255; Pozycja wykazu zwrotu w danym indeksie.

4383

4384 6.4.2.2 Uzyskiwanie (GET) odpowiedzi atrybutu PIB

4385 Te dane wysyłane są z urządzenia zgodnego z niniejszą specyfikacją w odpowiedzi na zapytanie jednego lub
 4386 więcej atrybutów PIB. Jeśli określony kwerendowany atrybut PIB nie jest utrzymywany na urządzeniu,
 4387 powinien on nadal odpowiadać na polecenie za pomocą pola wartości zawierającego w odpowiedzi same 1-
 4388 nki.

4389 Format treści pokazano na kolejnym rysunku.



4390

4391 **Rys. 105. Uzyskiwanie (GET) odpowiedzi atrybutu PIB. Treść**

4392 Pola żądania GET streszczone zostały w tabeli poniżej:

4393 **Tabela 119 - Pola odpowiedzi atrybutu PIB GET**

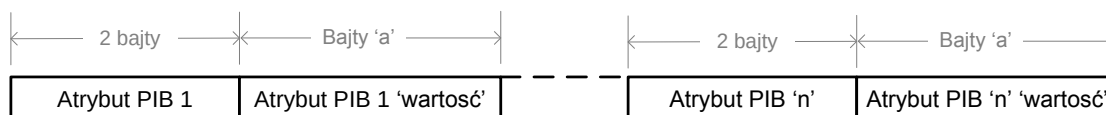
Nazwa	Długość	Opis
PIB Attribute id	2 bajty	16-bitowy identyfikator atrybutu PIB.
Index	1 bajt	Indeks pozycji zwróconych dla odpowiedniego identyfikatora Atrybutu PIB. To pole jest prawidłowe jedynie podczas zwracania atrybutów listy bazy informacji PLC. index = 0; jeśli atrybut PIB nie jest listą. Index = 1 do 255; Pozycja wykazu zwrotu w danym indeksie.
PIB Attribute value	„a” bajtów	Wartości żadanego atrybutu PIB. W przypadku listy atrybutów wartość składa się z całego rekordu odpowiadające danemu indeksowi atrybutu PIB.

Nazwa	Długość	Opis
Next	1 bajt	Indeks następnego wpisu zwróconego dla odpowiedniego identyfikatora atrybutu PIB. To pole jest prawidłowe jedynie podczas zwracania atrybutów listy bazy informacji PLC. kolejny = -0; jeśli atrybut PIB nie jest listą lub jeśli po atrybucie PIB nie występują żadne rekordy, tj. dany rekord jest ostatnim rekordem na liście. kolejny = 1 do 255; indeks kolejnego rekordu na liście jest zarządzany dla danego atrybutu PIB.

4394 Odpowiedź na zapytanie atrybutu PIB może rozciągać się pomiędzy kilkoma GPDU MAC. Ma to zawsze
 4395 miejsce, gdy odpowiedź zapytania połączonych (kilkunastu) atrybutów PIB jest dłuższa niż maksymalny rozmiar
 4396 segmentu dozwolony do przeniesienia przez zerową podwarstwę SCSS.

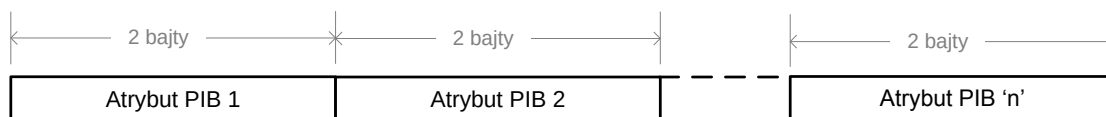
4397 6.4.2.3 Ustawianie atrybutu PIB

4398 Te dane zarządzania powinny być stosowane do ustawiania określonych atrybutów PIB. Taka treść
 4399 zarządzania składa się z 2-bajtowego identyfikatora atrybutu PIB, po którym następuje odpowiedniej
 4400 długości informacja o atrybucie PIB odpowiadająca temu identyfikatorowi. Ze względu na skuteczność
 4401 możliwe powinno być łączenie polecenia SET w kilku atrybutach PIB w jednej jednostce GPDU. Format
 4402 takiej połączonej treści przedstawiono na rysunku poniżej:



4403

4404 W przypadkach, gdy odpowiedni atrybut PIB jest jedynie wyzwalaczem (wszystkie atrybuty działań PIB), nie
 4405 powinno być żadnych wartości powiązanych, a format żądania danych powinien wyglądać następująco:



4406

4407 Zakłada się, że jednostka zarządzająca wysyłająca te informacje już ustaliła czy odpowiadające atrybuty są
 4408 obsługiwane w urządzeniu docelowym. Może zostać to osiągnięte poprzez poprzednie zapytanie i
 4409 odpowiedź na nie.

4410 6.4.2.4 Zerowanie statystyk

4411 Polecenie ma opcjonalną treść. W przypadku, gdy nie ma żadnej powiązanej treści, urządzenie odbierające
 4412 powinno zresetować wszystkie atrybuty statystyczne PIB.

4413 W przypadkach, gdy jednostka zdalnego zarządzania chce jedynie wykonać reset selektywnych atrybutów
 4414 statystycznych PIB, treść powinna zawierać listę atrybutów, które należy zresetować. Format powinien być
 4415 taki sam jak pokazano w punkcie 6.4.2.1

Ponieważ z urządzenia nie powraca żaden komunikat spełniający niniejszą specyfikację, jednostka zarządzająca musi wysłać uzupełniające zapytanie atrybutowe jeśli chce potwierdzić udane zakończenie odpowiedniego działania.

6.4.2.5 Ponowne uruchamianie urządzenia

Nie ma odpowiedniej treści związanej z tym poleceniem. Polecenie to jest kompletne samo w sobie. Urządzenie odbierające zgodne z niniejszą specyfikacją powinno się ponownie uruchomić po otrzymaniu tego komunikatu.

Obsługa tego polecenia i wszystkich powiązanych z nim działań jest obowiązkowa dla wszystkich implementacji zgodnych z tą specyfikacją.

6.4.2.6 Aktualizacja oprogramowania sprzętowego

W tym przypadku treść powinna zawierać polecenia aktualizacji oprogramowania sprzętowego i odpowiedzi opisane w punkcie 6.3 niniejszej specyfikacji.

6.4.3 Profil komunikacji zerowej warstwy SSCS

Ten profil komunikacji umożliwia wymianę informacji zarządzania opisanych w poprzednich punktach w zerowej podwarstwie SSCS.

Jednostki zarządzania zarówno na końcu odbierającym, jak i końcu wysyłającym to aplikacje wykorzystujące zerową podwarstwę SSCS opisaną w punkcie 5.3 niniejszej specyfikacji. Dane są zatem wymieniane jako Ogólne jednostki danych protokołu MAC.

6.4.4 Profil komunikacji szeregowej

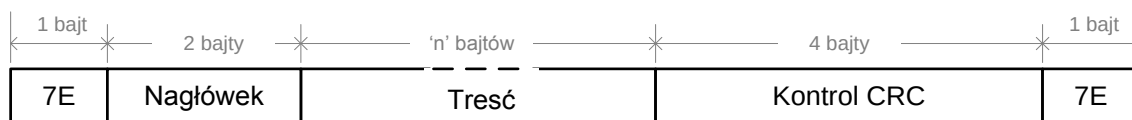
6.4.4.1 Warstwa fizyczna

Warstwa PHY może być dowolnym łączem szeregowym (np. RS232, szeregowo USB). Port szeregowy jest wymagane do konfiguracji 8N1 przy jednej z następujących prędkości danych:

9600 b/s, 19200 b/s, 38400 b/s, 57600 b/s

6.4.4.2 Hermetyzacja danych dla komunikatów zarządzania

Aby zapewnić odporność w ramach typu HDLC zamykany jest strumień danych, który obejmuje 2-bajtowy nagłówek i 4-bajtową kontrolę CRC. Wszystkie dane zawarte są pomiędzy początkową flagą bajta 0x7E a końcową flagą bajta 0x7E jak pokazano na rysunku poniżej:



4443

Rys. 106 – Hermetyzacja danych dla komunikatów zarządzania

Jeżeli którykolwiek ze znaków pośrednich danych ma wartość 0x7E, poprzedzany jest on bajtem Esc 0x7D, po którym następuje bajt wyprowadzony z oryginalnego znaku XORing z bajtem 0x20. Taka sama sytuacja ma miejsce, jeśli w ciągu znaków pojawiają się znaki 0x7D. Przykład takiego przypadku pokazano poniżej:

4448 Msg do Tx: 0x01 0x02 0x7E 0x03 0x04 0x7D 0x05 0x06

4449 Rzeczywista sekwencja Tx: 0x01 0x02 0x7D 0x5E 0x03 0x04 0x7D 0x5D 0x05 0x06

4450 Sekwencja Esc Sekwencja Esc

4451 32-bitowa kontrola CRC na końcu ramki obejmuje zarówno pola *Nagłówek* i *Treść*. Kontrola CRC obliczana
4452 jest przez pierwotne dane, które mają zostać wysłane, tj. przed przeprowadzeniem wypełniania wyżej
4453 opisanej sekwencji Esc bajtami. Obliczenia CRC:

4454 Wielomian wejściowy $M(x)$ ma postać wielomianu którego współczynniki są sprawdzanymi bitami danych
4455 (pierwszy bit do sprawdzenia jest najwyższym współczynnikiem korelacji, a ostatni bit do sprawdzenia jest
4456 współczynnikiem korelacji zerowej. Wielomian generujący dla kontroli CRC wynosi
4457 $G(x)=x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^5+x^4+x^2+x+1$. Reszta $R(x)$ jest obliczona jako reszta z
4458 dzielenia $M(x) \cdot x^{32}$ przez $G(x)$. Współczynniki reszty będą następnie wynikową kontrolą CRC.

4459 6.5 Lista obowiązkowych atrybutów PIB

4460 6.5.1 Ogólne

4461 Atrybuty PIB wymienione w tym punkcie są obsługiwane przez wszystkie implementacje. Atrybuty PIB,
4462 które nie są wymienione w tym punkcie są opcjonalne, a dostawcy mogą je wdrożyć wedle własnego
4463 uznania. Poza atrybutami PIB obsługiwane powinno być również polecenie ponownego uruchamiania
4464 określonych urządzeń (jak określono w 6.4.2.5).

4465 6.5.2 Obowiązkowe atrybuty PIB wspólne dla wszystkich typów urządzeń.

4466 6.5.2.1 Atrybut PIB warstwy PHY

4467 (Patrz Tabela 90)

4468 Tabela 120 - wspólne obowiązkowe atrybuty warstwy fizycznej PHY

Nazwa atrybutu	ID
phyStatsRxTotalCount	0x00A4
phyStatsBlkAvgEvm	0x00A5
phyEmaSmoothing	0x00A8

4469 6.5.2.2 Atrybuty PIB MAC

4470 (Patrz Tabela 92, Tabela 94 i Tabela 95)

4471 Tabela 121 - Wspólne atrybuty obowiązkowe PIB MAC

Nazwa atrybutu	ID
macEMASmoothing	0x0019

4472

Nazwa atrybutu	ID
MacCapabilities	0x002C

4473

Nazwa atrybutu listy	ID
macListPhyComm	0x0057

4474 **6.5.2.3 Atrybuty PIB aplikacji**

4475 (Patrz Tabela 98)

4476 Tabela 122 - Wspólne atrybuty obowiązkowe PIB aplikacji

Nazwa atrybutu	ID
<u>AppFwVersion</u>	0x0075
<u>AppVendorId</u>	0x0076
<u>AppProductId</u>	0x0077

4477

4478 **6.5.3 Obowiązkowe atrybuty węzła podstawowego**4479 **6.5.3.1 Atrybuty PIB MAC**

4480 (Patrz Tabela 92 i Tabela 96)

4481 Tabela 123 - Atrybuty obowiązkowe węzła podstawowego PIB MAC

Nazwa atrybutu	ID
macBeaconsPerFrame	0x0013

4482

Nazwa atrybutu listy	ID
macListRegDevices	0x0050
macListActiveConn	0x0051

4483 **6.5.4 Obowiązkowe atrybuty węzła serwisowego**4484 **6.5.4.1 Atrybuty PIB MAC**

4485 (Patrz Tabela 94, Tabela 96 i Tabela 97)

4486

Tabela 124 - Atrybuty obowiązkowe węzła serwisowego PIB MAC

Nazwa atrybutu	ID
macLNID	0x0020
MacLSID	0x0021
MacSID	0x0022
MacSNA	0x0023
MacState	0x0024
MacSCPLength	0x0025
MacNodeHierarchyLevel	0x0026
MacBeaconSlotCount	0x0027
macBeaconRxSlot	0x0028
MacBeaconTxSlot	0x0029
MacBeaconRxFrequency	0x002A
MacBeaconTxFrequency	0x002B

4487

Nazwa atrybutu listy	ID
macListSwitchTable	0x0053
macListAvailableSwitches	0x0056

4488

Nazwa atrybutu	ID
MACActionTxData	8
MACActionConnClose	8
MACActionRegReject	8
MACActionProReject	8
MACActionUnregister	8

4489

6.5.4.2 Atrybuty PIB aplikacji

4490

(Patrz Tabela 99)

4491

Tabela 125 - Atrybuty obowiązkowe węzła serwisowego APP PIB

Nazwa atrybutu	ID
<u>AppFwdlRunning</u>	0x0070
<u>AppFwdlRxPktCount</u>	0x0071

4492

Załącznik A
(informacyjny)
Przykłady kontroli CRC

Poniższa tabela podaje CRC obliczoną dla kilku określonych ciągów.

Tabela 126 – Przykłady CRC obliczonej dla różnych ciągów ASCII

Ciąg	CRC-8
'T'	0xab
"THE"	0xa0
0x03, 0x73	0x61
0x01, 0x3f	0xa8
„123456789”	0xf4

Załącznik B
(normatywny)
Obliczenia EVM

4499
4500
4501

4502 Niniejszy załącznik opisuje obliczenia EVM przez odbiornik referencyjny, przy założeniu dokładnej
4503 synchronizacji i rozmieszczenia okien FFT. Niech

- 4504 • $\{r_k^i; k = 1, 2, \dots, 97\}$ oznacza wartości wyjściowe FFT dla symbolu i , a k oznacza ton częstotliwości.
- 4505 • $\Delta b_k \in \{0, 1, \dots, M-1\}$ stanowi decyzję w sprawie otrzymanego symbolu informacji
- 4506 zakodowanego w przyroście fazy.
- 4507 • $M = 2, 4$, lub 8 w przypadku DBPSK, DQPSK lub D8PSK odpowiednio.
- 4508

4509 Wielkość wektora błędu określana jest następująco:

$$EVM = \frac{\sum_{i=1}^L \sum_{k=2}^{97} \left(\text{abs}(r_k^i - r_{k-1}^i e^{-(j*2*\pi/M) \times \Delta b_{k-1}}) \right)^2}{\sum_{i=1}^L \sum_{k=2}^{97} \left(\text{abs}(r_k^i) \right)^2}$$

4510

4511 W powyższym $\text{abs}(\cdot)$ odnosi się do wielkości liczby zespolonej. L to liczba symboli OFDM w treści jednostek
4512 PPDU odebranych jako ostatnie, na bazie których obliczana jest wielkość wektora błędu.

4513 SNR jest następnie określany jako wielkość odwrotna EVM.

4514

4515
4516
4517

4518

Załącznik C
(informacyjny)
Matryce przeplatania

Tabela 127 - Matryca przeplatania nagłówka.

12	11	10	9	8	7	6	5	4	3	2	1
24	23	22	21	20	19	18	17	16	15	14	13
36	35	34	33	32	31	30	29	28	27	26	25
48	47	46	45	44	43	42	41	40	39	38	37
60	59	58	57	56	55	54	53	52	51	50	49
72	71	70	69	68	67	66	65	64	63	62	61
84	83	82	81	80	79	78	77	76	75	74	73

4519

4520

Tabela 128 - Matryca przeplatania DBPSK(FEC WŁ.).

12	11	10	9	8	7	6	5	4	3	2	1
24	23	22	21	20	19	18	17	16	15	14	13
36	35	34	33	32	31	30	29	28	27	26	25
48	47	46	45	44	43	42	41	40	39	38	37
60	59	58	57	56	55	54	53	52	51	50	49
72	71	70	69	68	67	66	65	64	63	62	61
84	83	82	81	80	79	78	77	76	75	74	73
96	95	94	93	92	91	90	89	88	87	86	85

4521

4522

Tabela 129 - Matryca przeplatania DQPSK(FEC WŁ.).

12	11	10	9	8	7	6	5	4	3	2	1
24	23	22	21	20	19	18	17	16	15	14	13
36	35	34	33	32	31	30	29	28	27	26	25
48	47	46	45	44	43	42	41	40	39	38	37
60	59	58	57	56	55	54	53	52	51	50	49
72	71	70	69	68	67	66	65	64	63	62	61
84	83	82	81	80	79	78	77	76	75	74	73
96	95	94	93	92	91	90	89	88	87	86	85
108	107	106	105	104	103	102	101	100	99	98	97
120	119	118	117	116	115	114	113	112	111	110	109
132	131	130	129	128	127	126	125	124	123	122	121
144	143	142	141	140	139	138	137	136	135	134	133
156	155	154	153	152	151	150	149	148	147	146	145
168	167	166	165	164	163	162	161	160	159	158	157
180	179	178	177	176	175	174	173	172	171	170	169
192	191	190	189	188	187	186	185	184	183	182	181

4523

4524

Tabela 130 - Matryca przeplatania D8PSK(FEC WŁ.)

18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
36	35	34	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19
54	53	52	51	50	49	48	47	46	45	44	43	42	41	40	39	38	37
72	71	70	69	68	67	66	65	64	63	62	61	60	59	58	57	56	55
90	89	88	87	86	85	84	83	82	81	80	79	78	77	76	75	74	73
108	107	106	105	104	103	102	101	100	99	98	97	96	95	94	93	92	91
126	125	124	123	122	121	120	119	118	117	116	115	114	113	112	111	110	109
144	143	142	141	140	139	138	137	136	135	134	133	132	131	130	129	128	127
162	161	160	159	158	157	156	155	154	153	152	151	150	149	148	147	146	145
180	179	178	177	176	175	174	173	172	171	170	169	168	167	166	165	164	163
198	197	196	195	194	193	192	191	190	189	188	187	186	185	184	183	182	181
216	215	214	213	212	211	210	209	208	207	206	205	204	203	202	201	200	199
234	233	232	231	230	229	228	227	226	225	224	223	222	221	220	219	218	217
252	251	250	249	248	247	246	245	244	243	242	241	240	239	238	237	236	235
270	269	268	267	266	265	264	263	262	261	260	259	258	257	256	255	254	253
288	287	286	285	284	283	282	281	280	279	278	277	276	275	274	273	272	271

4525

4526

4527
4528
4529

Załącznik D
(normatywny)
Stałe warstwy MAC

4530 Niniejszy punkt określa wszystkie stałe warstwy MAC.

4531 **Tabela 131 - Tabela stałych MAC**

Stała	Wartość	Opis
MACBeaconLength	4 symbole	Długość sygnału w symbolach.
MACMinSCPLength	64 symbole	Minimalna długość SCP.
MACPriorityLevels	4	Liczba poziomów priorytetów obsługiwanych przez system.
MACCFPMalloc	32	Maksymalne okresy bezkolizyjnego dostępu, które mogą być przypisane w ramce.
MACFrameLength	276 symboli	Długość ramki podawana w liczbie symboli
MACRandSeqChgTime	32767 sekund (około 9 godzin)	Maksymalny czas, po którym węzeł podstawowy powinien rozesłać nową losową sekwencję do podsieci dla funkcji szyfrowania.
MACMaxPRNIgnore	3	Maksymalna liczba komunikatów wymaganych do promocji, którą może zignorować terminal.
$N_{\text{miss-beacon}}$	5	Liczba razy, gdy węzeł serwisowy nie otrzymał oczekiwanego sygnału przed uznaniem jego węzła serwisowego za niedostępny.
ARQMaxTxCount	5	Maksymalna liczba transmisji przed uznaniem trwałego niepowodzenia.
ARQCongClrTime	2 sek.	Jeśli odbiornik wskazał przeciążenie, należy odczekać ten czas przed ponownym przesłaniem danych.
ARQMaxCongInd	7	Gdy ARQMaxCongInd kolejnych transmisjach, które zakończyły się niepowodzeniem z powodu przeciążenia, połączenie należy określić jako trwale nieczynne.
ARQMaxAckHoldTime	7 sek.	Czas, o jaki odbiornik może opóźnić wysyłanie zatwierdzenia ACK w celu umożliwienia konsolidacji zatwierdzeń lub nakładania na zatwierdzenia ACK pakietów danych.

Załącznik E
(normatywny)
Stałe warstwy konwergencji

Poniższe wartości typu TYPE określone są do wykorzystania przez warstwy konwergencji z punktu 5.

Tabela 132 - Przydziały wartości TYPE

Nazwa symboliczna TYPE	Wartość
TYPE_CL_IPv4_AR	1
TYPE_CL_IPv4_UNICAST	2
TYPE_CL_432	3
TYPE_CL_MGMT	4
TYPE_CL_IPv6_AR	5
TYPE_CL_IPv6_UNICAST	6

Poniższe wartości LCID mają zastosowanie do połączeń broadcast definiowanych przez warstwy konwergencji z punktu 5.

Tabela 133 - Przydziały wartości LCID

Nazwa symboliczna LCID	Wartość	Zakres MAC
LCI_CL_IPv4_BROADCAST	1	Broadcast.
LCI_CL_432_BROADCAST	2	Broadcast.

Poniższe wartości wynikowe określone są dla prymitywów warstwy konwergencji.

Tabela 134 - Wartości wynikowe dla prymitywów warstwy konwergencji

Result (Wynik)	Opis
Success = 0	Usługa SSCS została pomyślnie przeprowadzona.
Reject = 1	Usługa SSCS nie powiodła się, ponieważ została odrzucona przez węzeł podstawowy.
Timeout = 2	Przekroczony limit czasu występuje podczas przetwarzania usługi SSCS
Not Registered = 6	Węzeł serwisowy nie jest teraz zarejestrowany w podsieci.

Załącznik F
(normatywny)
Profile

4543
4544
4545

4546 Biorąc pod uwagę różne aplikacje, które są przewidziane dla tych produktów zgodnych z niniejszą
4547 specyfikacją, konieczne jest zdefiniowanie różnych profili. Profile obejmują funkcjonalności, które
4548 reprezentują określony zestaw funkcji. Muszą one być realizowane zgodnie z zapisem zapewniania
4549 interoperacyjności.

4550 Niniejsza specyfikacja posiada kilka opcji, które, jeśli traktowane są w różny sposób przez różnych
4551 dostawców, utrudnią zarówno działania kontroli zgodności i współdziałanie przyszłych produktów. Profile
4552 dodatkowo ograniczają te opcje, tak aby promować interoperacyjność i testowalność.

4553 Określony profil zadecyduje które uprawnienia węzeł negocjuje przez procesy rejestracji i promocji.

4554 **F.1 Profil pomiaru inteligentnego**

4555 Następujące opcje będą albo obowiązkowe lub opcjonalne dla pomiarów inteligentnych.

4556 REG.CAP_SW:

- 4557 • Węzeł podstawowy: Ustawiony na 1.
- 4558 • Węzeł serwisowy: Ustawiony na 1.

4559 REG.CAP_PA:

- 4560 • Węzeł podstawowy: opcjonalnie.
- 4561 • Węzeł serwisowy: opcjonalnie.

4562 REG.CAP_CFP:

- 4563 • Węzeł podstawowy: opcjonalnie.
- 4564 • Węzeł serwisowy: opcjonalnie.

4565 REG.CAP_DC

- 4566 • Węzeł podstawowy: opcjonalnie.
- 4567 • Węzeł serwisowy: opcjonalnie.

4568 REG.CAP_MC

- 4569 • Węzeł podstawowy: Ustawiony na 1.
- 4570 • Węzeł serwisowy: opcjonalnie.

4571 REG.CAP_PRM

- 4572 • Węzeł podstawowy: Ustawiony na 1.
- 4573 • Węzeł serwisowy: Ustawiony na 1.

4574 REG.CAP_ARQ

- 4575 • Węzeł podstawowy: opcjonalnie.
- 4576 • Węzeł serwisowy: opcjonalnie.
- 4577 PRO.SWC_DC
- 4578 • Węzeł serwisowy: opcjonalnie.
- 4579 PRO.SWC_MC
- 4580 • Węzeł serwisowy: opcjonalnie.
- 4581 PRO.SWC_PRM
- 4582 • Węzeł serwisowy: Ustawiony na 1.
- 4583 PRO.SWC_ARQ
- 4584 • Węzeł serwisowy: opcjonalnie.

4585 **Załącznik G**
 4586 **(informacyjny)**
 4587 **Lista wykorzystanych częstotliwości**

4588 Poniższa tabela podaje dokładne częstotliwości (w Hz) dla 97 podnośnych sygnału OFDM.

4589 **Tabela 135 – Lista wykorzystanych częstotliwości**

Lp.	Częstotliwość	Lp.	Częstotliwość
1	41992,18750		
2	42480,46875	50	65917,96875
3	42968,75000	51	66406,25000
4	43457,03125	52	66894,53125
5	43945,31250	53	67382,81250
6	44433,59375	54	67871,09375
7	44921,87500	55	68359,37500
8	45410,15625	56	68847,65625
9	45898,43750	57	69335,93750
10	46386,71875	58	69824,21875
11	46875,00000	59	70312,50000
12	47363,28125	60	70800,78125
13	47851,56250	61	71289,06250
14	48339,84375	62	71777,34375
15	48828,12500	63	72265,62500
16	49316,40625	64	72753,90625
17	49804,68750	65	73242,18750
18	50292,96875	66	73730,46875
19	50781,25000	67	74218,75000
20	51269,53125	68	74707,03125
21	51757,81250	69	75195,31250
22	52246,09375	70	75683,59375
23	52734,37500	71	76171,87500
24	53222,65625	72	76660,15625
25	53710,93750	73	77148,43750
26	54199,21875	74	77636,71875
27	54687,50000	75	78125,00000
28	55175,78125	76	78613,28125
29	55664,06250	77	79101,56250
30	56152,34375	78	79589,84375
31	56640,62500	79	80078,12500
32	57128,90625	80	80566,40625
33	57617,18750	81	81054,68750

Lp.	Częstotliwość	Lp.	Częstotliwość
34	58105,46875	82	81542,96875
35	58593,75000	83	82031,25000
36	59082,03125	84	82519,53125
37	59570,31250	85	83007,81250
38	60058,59375	86	83496,09375
39	60546,87500	87	83984,37500
40	61035,15625	88	84472,65625
41	61523,43750	89	84960,93750
42	62011,71875	90	85449,21875
43	62500,00000	91	85937,50000
44	62988,28125	92	86425,78125
45	63476,56250	93	86914,06250
46	63964,84375	94	87402,34375
47	64453,12500	95	87890,62500
48	64941,40625	96	88378,90625
49	65429,68750	97	88867,18750

4590 Podnośna nr 1 jest podnośną pilotową. Pozostałe podnośne to podnośne danych.

4591

Załącznik H
(informacyjny)
Informacyjny

4592
4593
4594

H.1 Wymiana danych pomiędzy równorzędnymi IP

4596 Przykład pokazuje wymianę prymitywów pomiędzy węzłem serwisowym (192.168.0.100/24) a węzłem
4597 podstawowym, gdy ten pierwszy chce wymienić pakiety IP z węzłem trzecim (192.168.0.101/24), którego
4598 adres IP jest w tej samej podsieci IP.

4599 Ten przykład dokonuje następujących założeń:

- 4600 • Podwarstwa SSCS IPv4 węzła serwisowego (192.168.0.100) nie istnieje, więc węzeł musi uruchomić
- 4601 SSCS IPv4 i zarejestrować swój adres IP w węźle podstawowym przed wymianą pakietów IP.
- 4602 • Węzeł serwisowy (192.168.0.101) zarejestrował już adres IP w węźle podstawowym.

4603 Kroki zilustrowane na kolejnej stronie to:

4604 1. Warstwa IPv4 węzła serwisowego (192.168.0.100) wywołuje prymityw CL_IPv4_ESTABLISH.request. Aby
4605 ustanowić warstwę SSCS IPv4, wymagane jest:

4606 a. Ustanowienie połączenia z węzłem podstawowym, aby wszystkie komunikaty konwersji adresu
4607 można było przez nie wymieniać.

4608 b. Poinformowanie warstwy MAC węzła serwisowego, że SSCS IPv4 jest gotowa do odbierania
4609 wszystkich pakietów broadcast. Proszę zauważyć różnicę między broadcast i multicast. Aby dołączyć
4610 do grupy multicast, węzeł serwisowy będzie musiał poinformować węzeł podstawowy grupy do
4611 której chce dołączyć. Przedstawiono to w części A.2

4612 2. Warstwa IPv4_, po ustanowieniu podwarstwy SSCS IPv4, musi zarejestrować swój adres IP w węźle
4613 podstawowym. Aby to zrobić, wykorzysta ona już ustanowione połączenie.

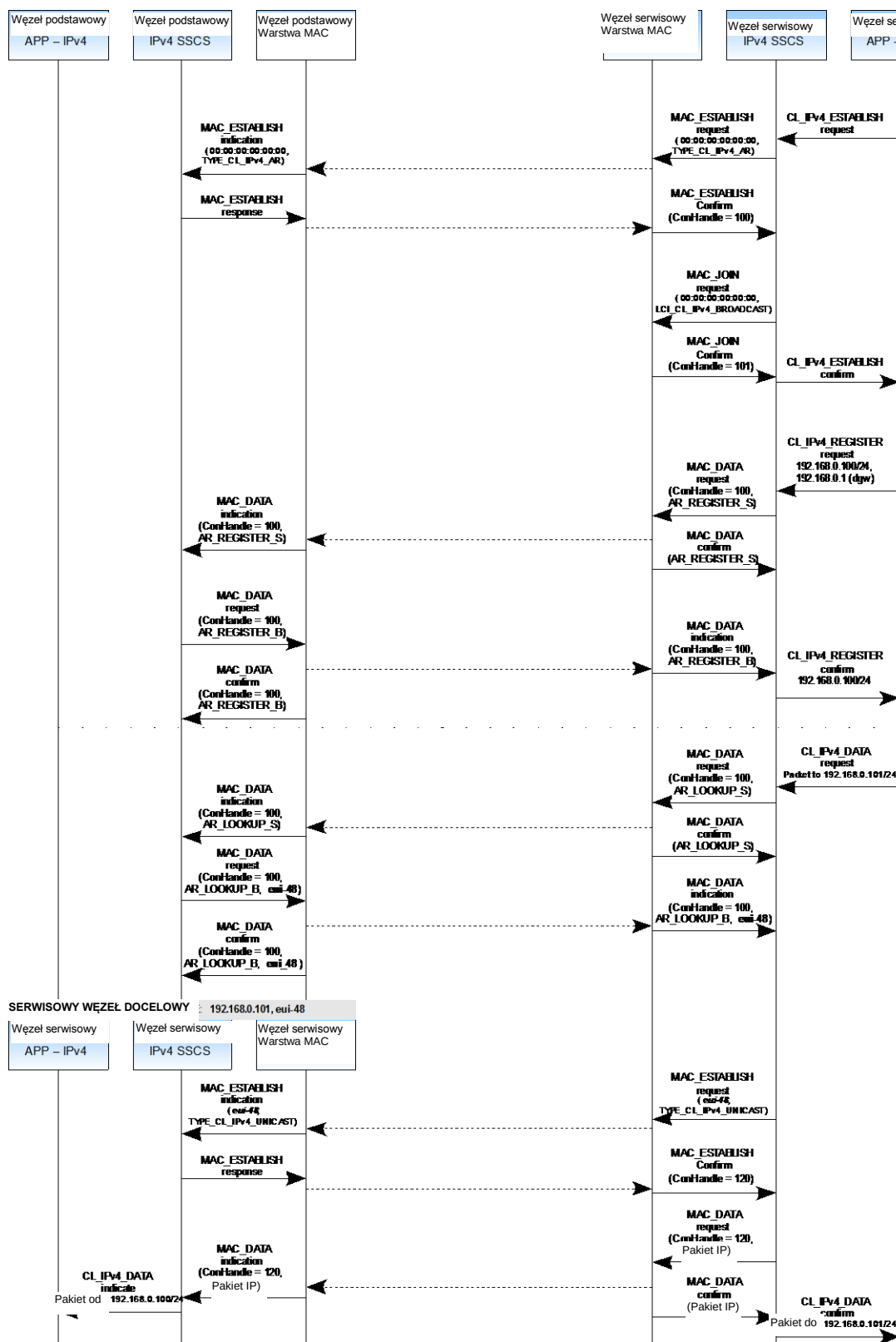
4614 3. Gdy tylko IPv4_ musi dostarczyć pakiet IPv4 do nowego adresu docelowego IP, należy wykonać poniższe
4615 dwa kroki (w tym przykładzie docelowy adres IP to 192.168.0.101).

4616 a. Ponieważ adres docelowy IPv4 jest nowy, podwarstwa SSCS IPv4 musi zażądać EUI-48
4617 skojarzonego z tym adresem. Aby to zrobić, komunikat żądania wyszukiwania wysyłany jest do węzła
4618 podstawowego.

4619 b. Po otrzymaniu EUI-48, nowe połączenie (typ = TYPE_CL_IPv4_UNICAST) jest ustanawiane, tak aby
4620 wszystkie pakiety IP do wymiany pomiędzy 192.168.0.100 i 192.168.0.101 korzystały z tego
4621 połączenia.

4622

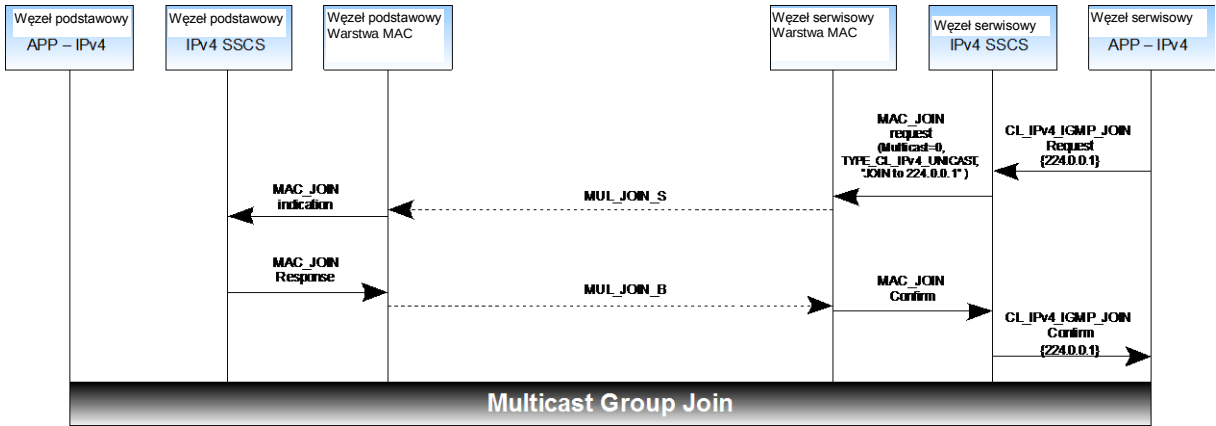
4623



Rys. H 1 - Usługi podwarstwy SCS IPv4

H.2 Dołączanie do grupy Multicast

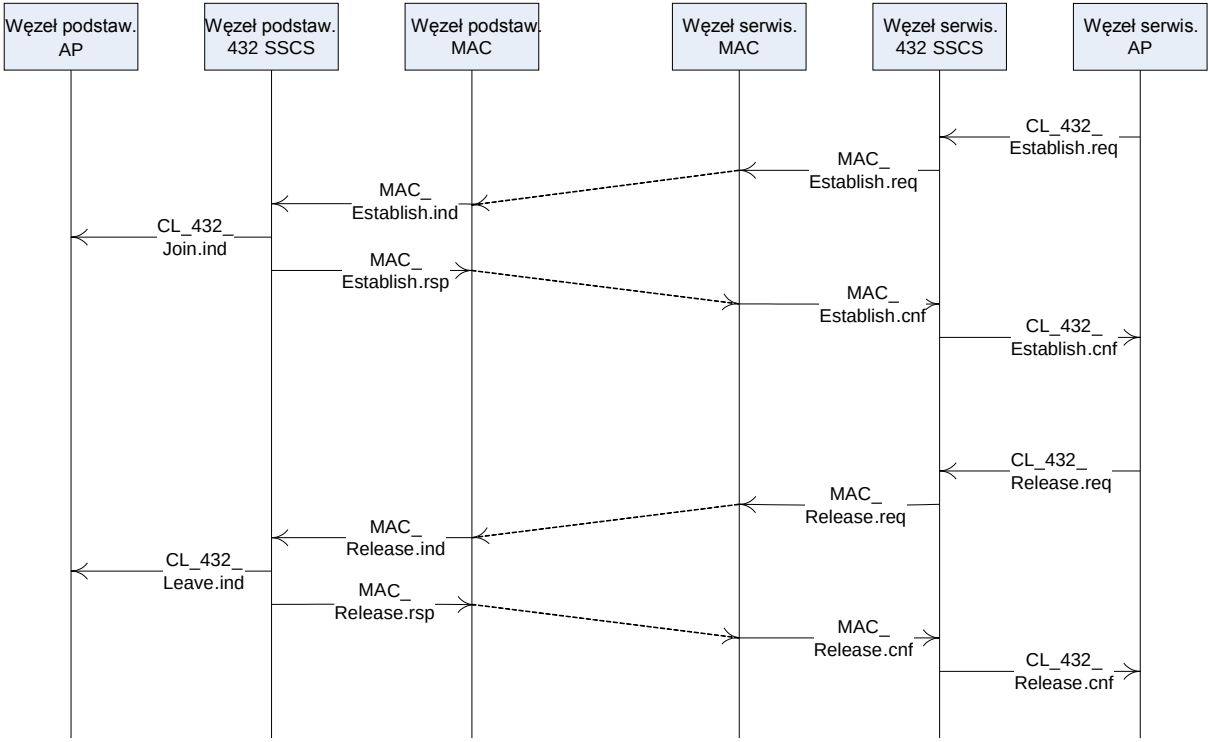
Rysunek poniżej przedstawia sposób dołączania węzła serwisowego do grupy multicast. Jak wspomniano wcześniej, główna różnica pomiędzy multicast i broadcast związana jest z wymienianymi komunikatami. W przypadku broadcast warstwa MAC będzie bezzwłocznie wysyłać prymityw MAC_JOIN.confirm, ponieważ nie musi ona wykonywać żadnych działań „od końca do końca”. W przypadku multicast prymityw MAC_JOIN.confirm wysyłany jest tylko, gdy sygnalizacja pomiędzy węzłem serwisowym, a węzłem podstawowym zostanie zakończona.



Rys. H 2 - Dołączanie

Poniższy diagram pokazuje ustanawianie i zwalnianie połączenia 432. Podwarstwa SSCS 432 dotyczy połączenia. Przed usługą 432_Data konieczne jest nawiązanie połączenia. Górna warstwa węzła serwisowego wysłała do podwarstwy 432 żądanie ustanowienia połączenia poprzez dostarczenie identyfikatora urządzenia jako parametru dla CL_432_Establish.request. Z pomocą usług warstwy MAC podwarstwa SSCS 432 węzła serwisowego wysłała żądanie ustanowienia połączenia do węzła podstawowego. Gdy ustanawianie połączenia powiedzie się, ten ostatni powiadamia górne warstwy, że węzeł serwisowy dołączył do sieci za pomocą prymitywu CL_432.Join.indication i dostarcza temu węzłowi serwisowemu adres docelowy podwarstwy SSCS poza własnym adresem SSCS za pomocą MAC_Establish.response, który przenosi te parametry.

Usługa CL_432_release kończy połączenie. Jest ona wysyłana przez górną warstwę węzła serwisowego do podwarstwy SSCS 432, która wykonuje ją z pomocą prymitywów warstwy MAC. Po stronie węzła podstawowego podwarstwa SSCS 432 powiadamia górną warstwę o zakończeniu połączenia poprzez CL_432_Leave.indication.



Rys. H 3 - Usługi podwarstwy SSCS 432

Załącznik I
(informacyjny)
Algorytm ARQ

4654
4655
4656

4657 Opisany tu algorytm jest tylko zaleceniem i ma na celu lepsze opisanie działania ARQ. Jednakże producenci
4658 mogą korzystać z innego algorytmu, o ile jest on zgodny ze specyfikacją.

4659 Gdy pakiet jest odbierany należy sprawdzić identyfikator pakietu. Jeśli jest to oczekiwany identyfikator i
4660 zawiera dane, powinien być przetwarzany w sposób normalny. Jeśli pakiet nie zawiera danych, może być
4661 odrzucony. Jeśli identyfikator nie jest zgodny z tym oczekiwanym i mieści się w oknie wejściowym, wtedy
4662 dla wszystkich pakietów nieotrzymanych z identyfikatorem, możemy założyć, że dane zostały utracone. Jeśli
4663 pakiet zawiera dane, dane te należy zapisać, aby przekazać je do warstwy konwergencji, gdy wszystkie
4664 pakiety zostały odebrane i przetworzone przez CL.

4665 Jeśli identyfikator pakietu nie mieści się w oknie wejściowym, możemy założyć, że jest to retransmisja, która
4666 została opóźniona i może być zignorowany.

4667 Jeśli występuje NACK, wszystkie pakiety z PKTID znajdujące się poniżej pierwszego NACK na liście zostały
4668 prawidłowo odebrane i mogą być usunięte z okna transmisji. Jeśli NACK nie występuje, a zamiast niego jest
4669 ACK, pakiety przed odebraniem ACK zostały odebrane i mogą zostać usunięte z okna transmisji. Wszystkie
4670 pakiety z listy NACK powinny być retransmitowane jak najszybciej.

4671 Są pewne sytuacje, gdy nadajnik ustawia bit resetujący, który może usprawnić ogólne działanie:

- 4672 • Gdy wypełnione jest okno albo nadajnika, albo odbiornika;
4673 • Na wyraźne żądanie warstwy CL;
4674 • Po przekroczeniu limitu czasu.

4675 Odbiornik nie ponosi odpowiedzialności za proces wysyłania zatwierdzeń w innym przypadku, niż gdy
4676 nadajnik ustawia bit resetujący. Mimo to kontroluje on przepływ. Z drugiej strony odbiornik jest w stanie
4677 wysłać ACK jeśli usprawnia to działanie ARQ w danym scenariuszu. Jednym z przykładów, stosowanym w
4678 wielu przypadkach, mogłoby być zmuszenie odbiornika do wysyłania ACK, jeśli okres czasu upłynął od
4679 ostatniego wysłanego zatwierdzenia, aby usprawnić wykorzystanie pasma (i ominąć zerowanie zegara w
4680 nadajniku). W tych sytuacjach nadajnik w dalszym ciągu odpowiada za współpracę z najprostszym
4681 odbiornikiem (który sam nie wysyła danych).

4682 Zaleca się, aby nadajnik pakietu ARQ zarządzał zegarem dla każdego niezatwierdzonego pakietu. Jeśli
4683 pakietu nie można prawidłowo zatwierdzić po upływie określonego czasu, pakiet zostanie ponownie
4684 przesłany. Ten rodzaj ponowienia wysyłania działa niezależnie od ponowień inicjowanych przez NACK. Po
4685 określonej ilości ponowień zaleca się aby rozłączyć połączenie. Mechanizm rozłączania ma na celu
4686 zapobieżenie ciągłemu ponawianiu przez węzeł pakietu ARQ. Dokładna liczba wartości ponowień zależy od
4687 własnego wyboru dostawcy.

4688	Lista autorów
4689	<i>Ankou, Auguste (Itron)</i>
4690	<i>Arribas, Miguel (Advanced Digital Design)</i>
4691	<i>Arzuaga, Aitor (ZIV)</i>
4692	<i>Arzuaga, Txetxu (ZIV)</i>
4693	<i>Berganza, Inigo (Iberdrola)</i>
4694	<i>Bertoni, Guido (STMicroelectronics)</i>
4695	<i>Bisaglia, Paola (ST Microelectronics)</i>
4696	<i>Cassin-Delaunier, Agnes (Texas Instruments)</i>
4697	<i>Estopinan, Pedro (Advanced Digital Design)</i>
4698	<i>Garai, Mikel (ZIV)</i>
4699	<i>Du, Shu (Texas Instruments)</i>
4700	<i>Garotta, Stefano (ST Microelectronics)</i>
4701	<i>Lasciandare, Alessandro (ST Microelectronics)</i>
4702	<i>Bois, Simone (ST Microelectronics)</i>
4703	<i>Liu, Weilin (CURRENT Technologies International)</i>
4704	<i>Llano, Asier (ZIV)</i>
4705	<i>Lunn, Andrew (CURRENT Technologies International)</i>
4706	<i>Miguel, Santiago (Advanced Digital Design)</i>
4707	<i>Pulkkinen, Anssi (CURRENT Technologies International)</i>
4708	<i>Rodriguez Roncero, Javier (Landis+Gyr)</i>
4709	<i>Romero, Gloria (Itron)</i>
4710	<i>Sánchez, Agustín (Landis+Gyr)</i>
4711	<i>Sanz, Alfredo (Advanced Digital Design)</i>
4712	<i>Schaub, Thomas (Landis+Gyr)</i>
4713	<i>Sedjai, Mohamed (CURRENT Technologies International)</i>
4714	<i>Sendin, Alberto (Iberdrola)</i>
4715	<i>Sharma, Manu (CURRENT Technologies International)</i>
4716	<i>Tarruell, Frederic(Itron)</i>
4717	<i>Teijeiro, Jesús (Advanced Digital Design)</i>
4718	<i>Varadarajan, Badri (Texas Instruments)</i>
4719	<i>Widmer, Hanspeter (CURRENT Technologies International)</i>
4720	<i>Wikiera, Jacek (CURRENT Technologies International)</i>
4721	